IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 42, No. 2, April, 2025, pp. 705-718
Journal homepage: http://iieta.org/journals/ts

CAA: Centrality Adapter Attack for Evaluating Smart City Resilience Against Targeted Attacks

Nouf Ali Alsowaygh*, Saleh Almowuena, Mohammed J.F. Alenazi, Maazen Alsabaan

Department of Computer Engineering, College of Computer and Information Sciences (CCIS), King Saud University, Riyadh 11451, Saudi Arabia

Corresponding Author Email: 441204614@student.ksu.edu.sa

https://doi.org/10.18280/ts.420209

Received: 24 September 2024
Revised: 21 January 2025
Accepted: 8 April 2025
Available online: 30 April 2025

Keywords:
smart city, network resilience, graph generator, network reliability, graph theory

ABSTRACT

Nowadays, increasing reliance on technology has driven the emergence of smart cities. Smart cities have made life much better for residents, improved resource management, Centrality operating costs considerably. In smart cities, there are many technologies used to sense, collect, and exchange data through networks. One of the main aspects that must be addressed in smart cities is the possibility of recovering the network and its services in case of failures, without human intervention. In this paper, we investigate the proper resilience network topology for smart cities. We evaluate the resilience of smart city network topology against three targeted attacks where we propose a new targeted attack, Centrality Adaptive Attack (CAA), to evaluate the robustness of network topology while the other attacks are betweenness centrality linked attack and degree-based link attack. The result of the experiment shows the degree-based attack is the more damaging targeted attack than the other, while CAA is the least harmful attack with low resilience. Finally, the result indicated the mesh network topology provides a better quality of service against those attacks.

1. INTRODUCTION

Nowadays, technology has expanded in all areas of life and has become a necessity in our daily lives due to the ease and affordability of hardware. Combining many aspects that have been extensively influenced by technology and have spread in recent times as a result of highly innovative Information and Communication Technology (ICT), the smart city has emerged. According to the United Nations, predicts that by 2050, 70% of cities are expected to be smart cities [1, 2]. The smart city is a concept that integrates information and communication technology with a range of physical items connected to an Internet of Things (IoT) network to enhance local operations and services and interact with citizens. Furthermore, local government officials may interact directly with the community and urban infrastructure, while also monitoring neighborhood activities and the growth of the city by means of smart city technology [3, 4].

Computer networks are considered the essential infrastructure for smart cities for generating, managing, and handling data and applications. Computer networks are being used to provide services for the majority of our daily activities. Smart city applications supported by the IoT rely on a variety of network topologies to create completely independent environments. IoT capillary networks serve small areas, such as BANs and wireless personal area networks. Examples include BANs, wireless personal area networks, and wireless local area networks (WPANs and WLANs). Street illumination, home automation, and indoor e-healthcare services are some of the application areas. On the other hand, wide area networks (WANs), metropolitan area networks (MANs), and mobile communication networks are used by applications such as ITS, mobile e-healthcare, and waste management. They are characterized in terms of data, size, coverage, latency, and capacity attributes [5].

There are different topologies for networks, with some being better than others in specific situations. When it comes to selecting the network's topology, managers have a variety of alternatives: in making their choice, they must consider the nature, size, goals, and budget of their business. Network topology management involves a range of activities, like configuration, visual mapping, and overall performance monitoring, and network topology has both a logical and a physical aspect. The physical topology illustrates the physical connections between nodes, such as wires and cables. In contrast, the logical topology explains the network's configuration and how the data flows. The design of a network is important for many reasons, as it is essential for the effectiveness of network operations. In addition to guaranteeing optimal network performance, the correct topology may make it simpler to spot problems, resolve issues, and more wisely distribute resources more wisely across the network [6, 7].

Smart cities are vulnerable to different types of attacks, including targeted attacks as well as natural disasters, which can disrupt their operations and services. Attacks on smart cities can be classified based on device property, adversary location, access level, attack procedure, host-based attacks, degree of information harm, or communication protocol stack [8]. In addition, the types of attacks can vary based on whether

it is a wireless sensor network (WSN) [9]. Figure 1 shows attacks that can affect a smart city with WSN [9].

Smart city services rely on advanced technologies like WSNs, Internet of Things (IoT), Cyber-Physical Systems (CPS), Robotics, and Unmanned Aerial Vehicles (UAVs), alongside robust networking and communication infrastructure. This provides the means for efficient message exchange between the different parts of a service [10]. Therefore, creating highly resilient networks is a critical element of their design and implementation. One of the factors that affect the network resilience is topology [11]. Network resilience against targeted attacks can be improved by adding more links in the network topology. The most resilient network is really produced by connecting links to create a full mesh, but this comes at an unaffordably high cost [12].

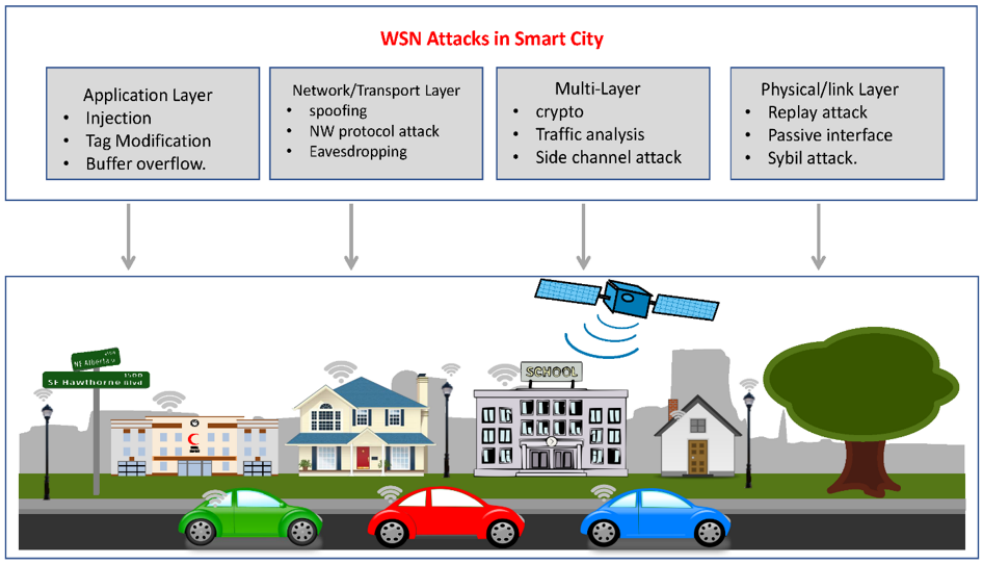

Figure 1. Types of attacks on a smart city with WSN

The contributions of this paper are summarized as follows:

- Proposed an approach that involves a novel targeted attack strategy, CAA, that adaptively selects links to attack based on two factors: node degree -how the node connected- and betweenness centrality- how nodes are important for flow of information-, providing a more comprehensively assess network resilience by analyzing network vulnerabilities.
- We determine the effectiveness of CAA through simulations on generated network topologies that mimic the characteristics of real-world smart city networks. Our results show that CAA can identify critical nodes and exploit vulnerabilities more effectively than degree-based or betweenness-based attacks alone.
- Based on the evaluation results, we provide practical guidelines for network designers to make smart city networks more resilient, considering factors such as topology selection and attack mitigation strategies. Where the CAA can be used as a tool to assess the resilience of existing or proposed smart city network topologies against targeted attacks.
- CAA simulations can be used to enhance smart city network resilience. This can be achieved by adding redundancy, protecting critical nodes, or redesigning the topology to minimize the impact of potential attacks.
- The CAA strategy serves as tool for network designers and to create more resilient smart city network that can tolerate targeted attacks.

The rest of this paper is organized as follows. In Section 2, background information regarding smart cities and network topology is provided. Section 2.1 outlines smart city architecture, applications, and characteristics. Section 2.2 discusses network resilience and the impacts of network topology and different attacks on their resilience. Section 3 review the related work that address smart city network resilience issues for different network. Section 4 talks about a proposed new attack and how it work. In Section 5, outlines discussion about the methodology and results. Section 6 presents our evaluation of network resilience in the smart city under different types of attack and different network topologies. Finally, Section 7 summarizes our findings and recommendations for further research.

2. BACKGROUND

This section presented a background about smart city network topology and the most common network attacks. Gaining unauthorized access to a company network with the intent to steal data or engage in other malicious behaviour is known as a network attack. The two primary categories of network attacks are passive and active. Network access allows passive attackers to monitor or steal sensitive data, but they cannot modify the data. Active attackers who gain unauthorised access can also alter data by deleting or encrypting it or doing other harm.

Typical attack methods that can be used by attackers to penetrate a network include taking advantage of weak passwords or insufficient protection against social engineering, while previously hacked accounts and insider threats add to the reasons for unauthorised access attacks. In Distributed Denial of Service (DDoS) attacks involve exploiting vast networks of compromised devices, known as botnets, to bombard servers or networks with illegitimate traffic. DDoS may take place on a network level, for example, by flooding the server with a large number of SYN/ACK packets, or at the application level, such as by executing complex SQL queries that completely destroy the database. In Man-in-the-Middle

(MITM) Attacks, involve attackers intercepting network traffic internally or externally. Attackers can intercept and steal data being transmitted, gain user credentials, and take over users' sessions if communication protocols are not protected. Another type of attack is code injection and SQL injection, where many websites accept user input without validating or cleaning it. Attackers can exploit input fields in forms or API call parameters to inject malicious code. Instead of entering or providing the expected data values, they inject code. When this code is processed by the server, it is executed, potentially allowing attackers to take control of the system and compromise network security [13].

2.1 Smart city

In this section, the smart city overview, architecture applications, and characteristics will be discussed. Smart cities increasingly incorporate networks, sensors, and computer-enabled software into buildings and infrastructure. Networks provide the energy for smart cities to improve how people live, work, and manage their everyday activities. In a smart city, people, devices, businesses, and governments must all be able to communicate securely, dependably, and rapidly. Thus, a Smart City approach should ensure that the increase in smart technology is accompanied by strategies to enhance performance, resilience, quality of service (QoS), or security. Therefore, the smart city is closely related to network resilience requirements and challenges.

2.1.1 Smart city architecture

There are many architectures to be considered in our research, as security and privacy are required against different attacks. Suitable architecture here is organized into four layers [14]. The Perception layer, also called the sensing layer or recognition layer, is responsible for collecting data and sending it to the Network layer. The second layer is the network layer whose responsibilities include establishing connections between servers, network devices, and smart objects, and ensuring the delivery of data gathered by the perception layer. The third layer is the support layer, which is responsible for supporting the needs of a various of applications through intelligent computing approaches. The last layer is the application layer, which is responsible for providing smart and useful services or applications to users according to their specific needs.

2.1.2 Smart city application

Application in smart city are classified into five categories. The goal of Smart Government is to provide improved services to citizens and communities through e-government services. Smart Transportation appears in traffic control, and smart parking. Smart Environment contributes to building a sustainable society and has the potential to predict natural disasters. Smart Utilities feature smart metering, smart grid, smart water meters, and smart light sensors. And finally, Smart Services include smart healthcare applications, remote control of home appliances, and smart shopping.

2.1.3 Smart city characteristics

A primary characteristic of a smart city is Het- erogeneity, which means the systems are widespread, independent, and accessed by many users. It refers to the presence of an extensive number of IoT nodes, communication protocols and technologies. Resource Constraints are important, as most IoT devices have limited resources; they inherently possess limited memory, battery capacity, and processing abilities. The RAM capacity and storage capabilities of these devices are usually limited. Mobility is not restricted to movement within the city and the delivery of goods from the source to the destination; it also includes technologies such as city-wide wireless communications and real-time traffic flow monitoring, as well as flexible responses to problems.

Connectivity means that any device has the potential to engage with the smart world. Scalability is a key characteristic in smart cities as they are expanding quickly, which may cause data and network traffic to grow at an accelerated rate; without scalable systems and methods, a smart city cannot operate effectively. User Involvement is crucial, since the primary goal of building smart cities is to serve the residents. Furthermore, citizen participation can enhance the quality of smart applications.

2.2 Network resilience

In this section, an overview will be provided of design and strategy, characteristics and challenges in relation to network resilience in smart cities. Network resilience is the system's ability to guarantee and maintain a sufficient level of service in spite of various failures and challenges that disrupt normal operation [15]. There are several features of network resilience, of which the following traits are the most crucial: security, availability, consistency, reliability, scalability, and recovery speed [16].

2.2.1 Design and framework

Design concepts affecting network resilience fall into four main groups: prerequisites, trade-offs, enablers, and behavior. The prerequisites for building a resilient system include five crucial requirements, such as identifying the amount of resilience that the system should offer, and defining metrics for measurement, while tradeoffs involve resources, complexity, and state management. Enablers con- sist of seven principles to guide the design, including self- protection and security, redundancy, diversity, and translucency. Lastly, behavior includes three concepts that govern the actions and characteristics of network resilience: namely, self-organization, adaptability, and evaluability.

The main element of the network resilience framework is the control loop; this can determine the other elements, such as resilience encompasses metrics, threat awareness, distributed information storage, and rules-based management and relies on real-time components of (D^2R^2+DR): defending, detecting, remediating, recovering, in addition to diagnosing and refining. Resilience control is carried out through these five steps. First, determine the targets of resilience: this takes into account the demands of service providers, network operators, and end users. Second, identify defensive measures responsible for infrastructure provisioning and self-protection services that are redundant and diversified. Third, identify challenges and describe them using a range of information sources. Fourth, a resilience estimator checks to see whether the resilience goal is being met, based on resilience metrics. Finally, a resilience manager controls resiliency mechanisms that are embedded in the network [17].

2.2.2 Topology and challenges

The design and configuration of a network that enables it to resist interruptions and continue to operate even in the face of

failures or assaults is referred to as network resilience topology. When designing a network to provide resilience, network topology is a crucial component [11]: it determines the network's ability to carry on even in the face of failures or assaults. There are a number of network resilience topologies, such as mesh topology, ring topology, star topology, or hybrid topology, that may be employed, and each has advantages and disadvantages.

Overall, network resilience topology should be chosen based on specific network needs and requirements. By designing a network with resilience in mind and selecting the appropriate topology, organizations can ensure that their networks can continue to function even in the face of disruptions or attacks [18, 19].

Understanding how different architectures, designs, and protocols respond to challenges is key to assessing network resilience and designing resilient net- works. Some of these challenges are natural disasters such as fire, earthquakes, hurricanes, or floods, attacks, environmental challenges, low-level service failures, and legitimate but unusual traffic.

2.2.3 Network resilience in smart city

This section discusses why network resilience is crucial for smart city functionality. In a smart city, network resilience is becoming increasingly important to prevent both attacks that cause failures in the network's weakest areas and major disasters that totally destroy part of the network [20]. It is a crucial component of modern urban planning, especially when creating smart cities [21]. Transportation, communications, electricity, water supply, and other linked networks are some of the networks that smart cities significantly rely on; a smart city and its economy cannot operate properly without them. However, they are exposed to interruptions driven by unexpected events like cyber-attacks and natural disasters. Several actions may be taken to improve network resilience in smart cities.

First, communities may spend money on redundant network infrastructure, such as communications and power backup to ensure that critical services are not disrupted during emergencies. Second, cities can leverage advanced technologies such as IoT to monitor network performance in real-time and detect anomalies or potential threats before they cause major disruption. This can help city officials to take proactive measures to prevent or mitigate impacts. Third, cities can engage in scenario planning exercises and develop contingency plans to respond to different types of disruptions. This can involve developing emergency response protocols and training personnel to handle crises effectively. Fourth, cities can foster community resilience by promoting citizen participation and engagement in disaster preparedness and recovery efforts. In summary, network resilience is a fundamental element in smart city planning, and cities should prioritize investments and initiatives that enhance the resilience of critical infrastructure networks. In this way, cities can minimize the impacts of disruptions and ensure that they continue to function effectively even in the face of unforeseen events [21, 22].

3. RELATED WORK

Ensuring network resilience is a cornerstone for maintaining and enhancing smart city. The network resilience is a priority due to ensuring services, adaptability to change, mitigating risks, data integrity and security, and service reliability [23, 24].

In this section review the related work done in to enhance smart city network resilience either through technique, topology, and attacked.

Syed et al. [25] introduced a comprehensive study of the IoT in smart cities. They began by talking about the essentials elements of the Internet of Things (IoT)-based Smart City landscape, then they explained the technologies that make the existence of these domains possible in terms of the architecture used, the network technologies employed, as well as the artificial algorithms used in smart city systems built on the Internet of Things. The authors reviewed the most common methods and applications across different Smart City domains. Moreover, they discussed the challenges that arise while deploying applications for smart cities and introduced some potential solutions. Finally, a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis was presented, along with a discussion of the security and privacy challenges facing smart cities based on the Internet of Things.

Estrada [26] showed that 40% of all networks have significant weaknesses that make them susceptible to targeted attacks. They used the graph spectral method and introduced a a new measurement for how well a network expands, called Good Expansion (GE). By means of this parameter they classified 51 real-world complex networks. The researcher divided these complex networks into four groups according to their GE characteristics and node Degree Distribution (DD), each of which is more or less resilient to targeted attacks on its nodes. The strength and robustness of complex networks are significantly enhanced through the coexistence of GE properties and uniform degree distribution.

Al-Zoman and Alenazi [27] proposed a new solution for net- works in smart cities. Software-Defined Networking (SDN) are used to provide Quality of Service (QoS) in case of a connection interruption. They tested their proposed solution using typical smart city data. The evaluation results showed that the proposed approach improves the productivity of critical applications during disconnection and achieves better service quality.

Jawhar et al. [10] described the networking requirements and characteristics of smart city applications, as well as the networking protocols that can be used to support the diverse data traffic flows required between different parts. Additionally, they showed some examples of the networking designs of some smart city systems, such as the smart grid, smart home energy management, smart water, pipeline monitoring and control systems.

Alenazi and Cetinkaya [28] introduced Nodal Disjoint Path (NDP), a metric quantifying a node's significance based on its diverse connectivity to other nodes. They suggested two NDP-based algorithms, NDP-global and NDP-cluster, to identify k controllers for improving network resilience to targeted attacks. They tested the robustness of the two selected algorithms against five centrality-based attacks and random failures on four fiber-level US networks. The evaluation results have been shown that selecting controllers using the NDP-global algorithm improves the network's resilience against centralization-based attacks and random failures compared to the NDP-cluster, k-median, and k-center algorithms. The results indicated that the NDP-cluster method gives higher accuracy and faster response times than the k-median technique.

Alablani and Alenazi [29] introduces a new dissemination

algorithm, the Delaunay Triangulation-based Dissemination Evaluation for Smart Cities (EDTD-SC). This algorithm focuses on sink placement, as well as sensor distribution. They used Delaunay triangulation and k-means clustering were employed in their algorithm to identify the best spots for increasing coverage while preserving connectedness and robustness when there are obstructions in the sensing region. The results showed that the EDTD-SC had improved area coverage and end-to-end latency. It outperformed random and routine deployments by 29.6% and 29.7%, respectively. Moreover, it demonstrated high performance in terms of resilience against attacks.

Alenazi [12] looked into how adding a cost-effective set of links might improve the resilience of real-world networks. A suitable solution was found through improving a graph resilience metric, such as algebraic connectivity or total graph diversity using a greedy approach, in which a set of links has been added to increase network connectivity. The researcher uses three centrality-based attacks to assess the upgraded networks and look at their resilience. The findings of the attacks on flow robustness indicated that enhanced networks were more resilient than non-improved networks.

Ibrahim et al. [30] suggested an adaptive aggregation solution to address IoT network challenges. With the use of these strategies, data can be abstracted, sending fewer packets so that there is no traffic congestion, and using less often-used packet headers. In order to investigate the simulation findings, the proposed adaptive aggregation techniques are implemented using IoT networks of smart city that have been tested architecturally and practically. In comparison to the current aggregation methodologies, it is projected that the outcomes of adaptive aggregation is projected to significantly improve the operational efficiency of IoT smart city networks across key performance indicators.

Marksteiner et al. [31] examined the most significant wireless IoT protocols for smart homes, which include KNX-RF, EnOcean, Zigbee, Z-Wave, and Thread, and provided an overview of IoT application domains. Finally, researchers examined the security attributes of the above protocols and summarized their differences, recommending which protocols are better suited for a safe smart home. All other protocols rely on less practical or safe methods, such as pre-shared or default keys, to secure the key exchange, unlike the thread protocol, despite being a less trusted curve.

Piraveenan et al. [32] developed a tool to evaluate the structural resilience of complex networks that is particularly useful in cases of targeted, ongoing attacks. The measurement is based on how the largest component changes in size as the network breaks down. They suggested that the measure can be used to evaluate and contrast the efficiency of different attack strategies. By using this metric, they were able to support the finding that scale-free networks are more vulnerable to targeted attacks than random attacks. Then, they examined the resilience of a variety of real-world networks, demonstrating that the majority of them are least resistant to attacks depending on the betweenness of nodes. Additionally, they have demonstrated that the robustness of some networks is more sensitive to the attack strategy than others, and that the presented robustness metric can be a crucial tool in selecting attack and defense strategies for real-world networks.

Huang [33] developed a wireless sensor network topology based on a neighbor graph. The researcher introduced the DV-Hop (Distance Vector-Hop) localization technique with average hop weighting and hop number correction. The shadowing model transforms the signal intensity value received by the node into the distance between the nodes; and the hop value is adjusted using the ratio of the distance between the nodes to the communication radius. The MDV-Hop (Modified Distance Vector-Hop) algorithm was developed to enhance the positioning performance and reduce the error due to the number of hops between anchor nodes. To find the coordinates of the unidentified node, the modified Bat algorithm was used in place of the greatest likelihood approach. The simulation showed that the DV-Hop localization algorithm based on Bat optimization can achieve higher localization accuracy and better stability.

Bhandari and Cho [34] suggested a parent selection strategy that is effective and avoids an overworked parent. The method uses numerous routing measures in combination to compute rank, which leads to balanced topology development and the most reliable routing for Advanced Metering Infrastructure (AMI) networks that use the Routing Protocol for Low-Power and Lossy Networks (RPL). By implementing the suggested strategy in the Contiki OS using the Cooja emulator. The simulation results demonstrated that, in com- parison to default RPL, the proposed strategy offers a greater packet delivery ratio, lower latency, and higher throughput.

Pasolini et al. [35] presented two smart city testbeds. The first involved a smart lighting infrastructure that was diverse and used IEEE 802.15.4 short-range communication technology. The second focused on applications for smart buildings and was built on the LoRa low-rate, long-range communication technology. Adaptable and modular installation of a public lighting infrastructure were covered in the smart lighting scenario. As the smart-building testbed was examined, measurement campaigns and simulations were used to gauge the performance and coverage of the LoRa technology in an actual urban setting. Results indicated that to effectively cover vast urban areas while keeping the airtime low enough to maintain acceptable packet loss levels, the right parameter settings were required. Long-range LoRa technology testing evidence demonstrated that its maximum coverage in a dense urban area was in the range of 1-2 km.

Table 1 provides a comparison of the studies we have presented. All the research discussed was about improving network performance in smart cities and the different techniques that are used to improve network resilience against different types of attacks, whether targeted or not in different type of network typologies. From that need more research focus in network topology for resilient network smart city against central attacks.

This paper focus in evaluate different smart city network topology against the central attacks which that affect the performance and resilience of network in smart city from this we proposed the CAA and test the performance of it after comparison it with two different targeted attacks to decide better network topology resilient for smart city.

To address these gaps, our paper focuses on evaluating mesh and hybrid network topologies for smart cities against centrality-based targeted attacks. We propose a novel Centrality Adaptive Attack (CAA) strategy that combines betweenness centrality and node degree using a weighting factor to identify critical links. By comparing the performance of CAA with other targeted attack strategies, we aim to determine the most resilient network topology for smart cities and provide insights for designing robust networks.

Our work complements existing research by providing a more comprehensive evaluation of mesh and hybrid network

topologies against targeted attacks. By considering multiple centrality measures and introducing a weighting factor in the CAA strategy, we offer a more nuanced approach to identifying critical links compared to studies that rely on single centrality measures. Furthermore, our comparative analysis of different targeted attack strategies provides valuable insights into the resilience of various network topologies, aiding in the design of robust smart city networks.

Table 1. Comparison of related works

Study	Year	Proposed Model/Technique	Technology Used	Failure Type	Topology	Result
Ibrahim et al. [30]	2022	Adaptive (Collocation OR Time) Aggregation techniques	Adaptive asynchronous distributed clustering algorithms, ML DL models	--------	Mesh	Reduced collision probability, and recurring overheads
Al-Zoman and Alenazi [27]	2020	Smart City Resilient System (SCRS)	SDN	Link Failure	Mesh	25% increase in Throughput
Alablani and Alenazi [29]	2020	EDTD-SC strategy	Delaunay triangulation, Voronoi diagram, and k-means	Degree and Betweenness-based attacks	--------	60% reduction in delay, and increase by 29.6% in area coverage.
Huang [33]	2020	DV-Hop MDV-Hop	Routing exchange protocol improved Bat algorithm	--------	Wireless sensor network topology	Higher positioning ac curacy and better stability
Alenazi and Cetinkaya [28]	2019	NDP-global NDP-cluster - algorithms based on NDPnodal metric	SDN	Centrality-based attacks Random Failures	4 Fiber-level topologies	Improvement in propagation delays
Bhandari and Cho [34]	2019	Routing Protocol for low power and Lossy Network (RPL)	Parent selection mechanism, and AMI network	--------	Resource efficient topology	Greater packet delivery ratio, lower latency, and higher throughput
Marksteiner et al. [31]	2017	IoT Protocols	KNX-RF, EnOcean, Zigbee, Z-Wave and Thread	--------	Star, Fully Connected, and Mesh	Z-Wave has strongest security building blocks.
Piraveenan et al. [32]	2012	Robustness coefficient measure	--------	Targeted, sustained attacks	--------	Coefficient measure is a valuable tool analysing networks.
Estrada [26]	2006	Parameter measures GEofNetwork	Graph topologies Spectral	Targeted Attacks Link Failure	--------	Lack in GE makes network vulnerable

4. PROPOSED CAA

In this section, we propose a new targeted attack strategy called CAA, which aims to select links to attack based on a combination of betweenness centrality and node degree. By considering both factors, CAA provides a more comprehensive approach to evaluating network resilience compared to attacks that focus on only one centrality measure.

Betweenness centrality measures how often a node lies on the shortest paths between other nodes in the network. Nodes with high betweenness centrality are critical for maintaining network connectivity and are often targeted in attacks. On the other hand, node degree represents the number of connections a node has, and high-degree nodes are also attractive targets for attackers looking to maximize disruption.

The CAA algorithm works as follows:

1. Calculate the betweenness centrality (BC) and node degree (ND) for all nodes in the network.
2. Normalize BC and ND values to the range [0, 1] to ensure equal weighting. For each link (i,j) in the network, calculate the CAA score as:

$$CAA(i,j) = \alpha \times BC(i) + (1 - \alpha) \times ND(j) \quad (1)$$

where, α is adaptable parameter that controls the relative importance of BC and ND.

3. Sort the links in descending order of their CAA scores. Select the top k links to attack, where k is a pre-determined attack budget.

The adaptable parameter α in the CAA algorithm plays an important role in determining the relative importance of betweenness BC and ND when selecting links to attack. By adjusting the value of α, network designers can prioritize either BC or ND, or consider both factors equally.

- When $\alpha = 1$, the CAA score is solely based on the normalized BC value of the source node i. This means that the attack strategy will prioritize links connected to nodes with high betweenness centrality, which are critical for maintaining network connectivity.
- When $\alpha = 0$, the CAA score is solely based on the normalized ND value of the target node j. In this case, the attack strategy will focus on links connected to high-degree nodes, which are hubs in the network and whose removal can cause significant disruption.
- When $0 < \alpha < 1$, the CAA score is a weighted combination of both BC and ND. The specific value of α determines the relative importance of each factor. For example, if $\alpha = 0.5$, both BC and ND are given equal weight in the link selection process.

In our experiments, we investigated the impact of different α values on the effectiveness of the CAA strategy. We considered three scenarios:

- BC-prioritized attack ($\alpha = 0.8$): This setting gives higher priority to links connected to nodes with high betweenness centrality.
- ND-prioritized attack ($\alpha = 0.2$): This setting gives higher priority to links connected to high-degree nodes.
- Balanced attack ($\alpha = 0.5$): This setting gives equal importance to both BC and ND in the link selection process.

By evaluating the network resilience under these different α values, we aim to provide insights into how the relative importance of BC and ND affects the effectiveness of the CAA strategy and its impact on smart city network topologies. The results of this analysis will be presented in Section 6.

The pseudocode of the algorithm developed to implement the proposed adaptive attack is provided in Algorithm 1. Algorithm 1 works as follows. Initially, define an empty list for sorting the selected links for attacks. for each node in the graph will calculate its betweenness centrality using and its node degree. Secondly, will Normalize the betweenness centrality values to the range [0, 1], and normalize the node degree values to the range [0, 1]. Then, for each link in the graph, calculate its CAA_score using the Eq. (1).

Algorithm 1
1: Algorithm: Centrality Adaptive Attack (CAA)
2: **Input:**
3: - Graph $G(V, E)$
4: - Number of links to attack (attack_budget)
5: - Tunable parameter (alpha)
6: **Output:**
7: - List of selected links to attack (attacked_links)
8:
9: **Procedure:**
10: Initialize attacked_links as an empty list
11: **for** each node n in V **do**
12: Calculate betweenness_centrality(n) using Brandes' algorithm
13: Calculate node_degree(n)
14: **end for**
15: Normalize betweenness_centrality values to the range [0, 1]
16: Normalize node_degree values to the range [0, 1]
17: **for** each link (i, j) in E **do**
18: Calculate CAA_score(i, j)= alpha × betweenness_centrality(i) + (1 - alpha) × node_degree(j)
19: **end for**
20: Sort links in descending order based on their CAA_score
21: **for** k = 1 to attack_budget **do**
22: Select link (i, j) with the kth highest CAA_score
23: Add link (i, j) to attacked_links
24: **end for**
25: **return** attacked_links
26:
27: Procedure betweenness_centrality(node):
28: - Implement Brandes' algorithm to calculate betweenness centrality
29: - Return betweenness centrality value for the given node
30:
31: *Procedure node_degree(node):*
32: - Calculate the degree of the given node
33: - Return the node degree value

Fourth, will Sort the links in descending order based on their CAA_score. Otherwise, will repeated from 1 to attack_budget in order to select the ink with highest CAA_score, then the selected link will be added it to the attacked_links list. Finally, will return the list of selected links to attack.

Here is an example to clarify the idea of the proposed centrality attack. Let's assume we have a smart city network topology with 8 nodes connected in a mesh topology, as shown in Figure 2. We calculate the betweenness centrality and node degree for each node, as shown in Table 2.

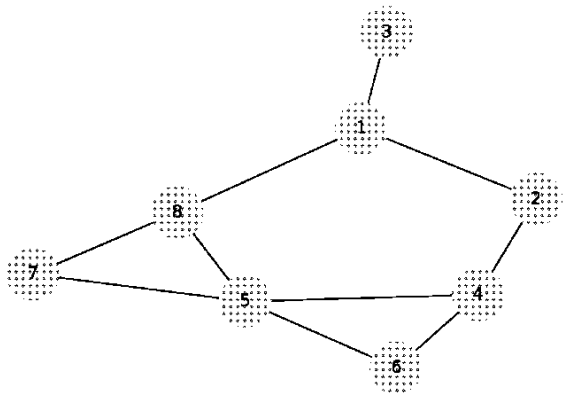

Figure 2 Example of smart city topology of CAA

Table 2. Example of CAA

Node	Betweenness Centrality	Node Degree
1	0.357	3
2	0.143	2
3	0.000012	1
4	0.167	3
5	0.261	4
6	0.00002	2
7	0.0000001	2
8	0.262	3

The calculation will find the node that has the maximum value of betweenness centrality, then check if another node has the same maximum value. If no other node is found, then this node will be attacked. Otherwise, if more than one node has the maximum value, which one will be attacked will be decided based on the degree value of the nodes; the one that has highest degree will be attacked. As shown in our example, in the first instance there is only one node with maximum betweenness centrality, which is node number 1, so this will be attacked first. Next, there are two nodes with maximum betweenness centrality, nodes 5 & 8: node 5 will be selected because it has the highest degree.

Then this node will be attacked. Otherwise, if more than one node has the maximum value, which one will be attacked will be decided based on the degree value of the nodes; the one that has highest degree will be attacked.

The CAA strategy is designed to adaptively combine betweenness centrality and node degree through a weighted parameter α. The motivation behind this approach is to consider both the global importance of nodes in terms of their role in shortest paths (betweenness centrality) and their local connectivity (node degree). By incorporating both centrality measures, CAA aims to identify critical links that have a significant impact on network connectivity and performance.

As shown in our example, in the first instance there is only one node with maximum betweenness centrality, which is node number 1, so this will be attacked first. Next, there are two nodes with maximum betweenness centrality, nodes 5 & 8: node 5 will be selected because it has the highest degree.

We get that the adaptive nature of CAA and its ability to consider multiple centrality measures provide a valuable tool for assessing the resilience of smart city networks against targeted attacks. The weighted parameter α allows for flexibility and customization, enabling network designers to tailor the attack strategy based on their specific security

priorities and network characteristics.

4.1 Computational complexity analysis

One important consideration of the CAA algorithm in large-scale smart city networks is its computational complexity and scalability. As the size of the network grows, calculating betweenness centrality and node degrees for all nodes and links can become computationally challenging. The time complexity of calculating betweenness centrality using Brandes' algorithm is O(NM) for unweighted networks and $O(NM + N^2 \log N)$ for weighted networks, where N is the number of nodes and M is the number of links [36].

To address scalability issues, we propose several strategies. Parallel and distributed computing techniques can be employed to distribute the computation across multiple nodes using frameworks like GraphX [37]. Approximation techniques, such as the Riondato and Kornaropoulos [38] and Geisberger et al. [39] algorithms, can estimate betweenness centrality with reduced computational overhead, providing a trade-off between accuracy and efficiency. For dynamic networks, incremental update algorithms like the Incremental Betweenness Centrality [40] and Incremental PageRank [41] algorithms can efficiently recompute centrality measures based on local changes.

We acknowledge that these strategies may have limitations and trade-offs, such as sacrificing accuracy for efficiency or not being suitable for all types of network changes. In our future work, we plan to investigate the applicability and effectiveness of these strategies in the context of smart city networks, evaluating the trade-offs between accuracy and efficiency. By incorporating these scalability strategies and considering their trade-offs, we aim to enhance the practical applicability of the CAA algorithm for large-scale smart city networks, enabling efficient analysis of network resilience and supporting the development of robust and scalable resilience strategies.

5. EVALUATION

In this section, we describe the characteristics of the smart city network topologies used in our study and the experimental setup for evaluating their resilience against targeted attacks. As our study does not rely on real-world smart city network data, we have generated our own network topologies based on common structures and properties observed in smart city networks.

5.1 Network topology

Here we present a small smart city network to study its behavior in the event of a link failure. The network configuration, or network topology, is a key factor in determining its performance. Network topology is the arrangement of the network, including the physical and logical description of how links and nodes are set up to communicate with each other. Network connectivity, ease of use, and uptime protection can be affected by how it is configured.

The choice of network topology plays a crucial role in determining the resilience of smart city networks against targeted attacks. By analyzing the performance of the mesh and hybrid topologies under different attack scenarios, we aim to provide insights into their strengths and vulnerabilities.

Here, an explanation of the categories of network topologies will be provided:

1. Mesh Topology: In a mesh topology, any node in the network can connect directly to any other node in the same network, as shown in Figure 3 illustrates the mesh topology, where nodes are interconnected, forming a dense and redundant network structure. Each node is connected to multiple neighboring nodes, creating multiple paths between any pair of nodes. This topology provides high resilience against node or link failures, as alternative routes are available.

2. Hybrid Tree-Star Topology: One node is known as the root node and is grouped with the other nodes in a hierarchical sequence, as shown in Figure 4 which combines a mesh backbone with tree-like subnetworks at the edge.

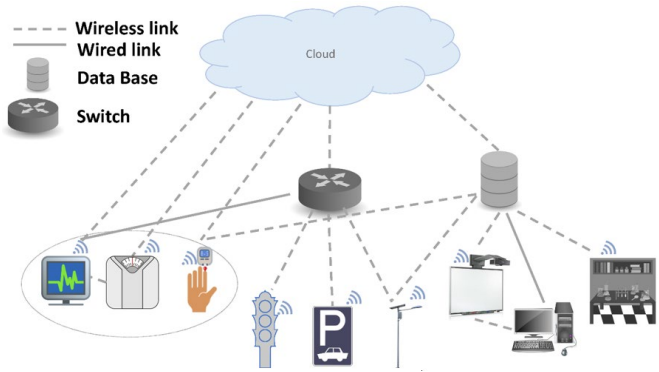

Figure 3. Mesh network topology

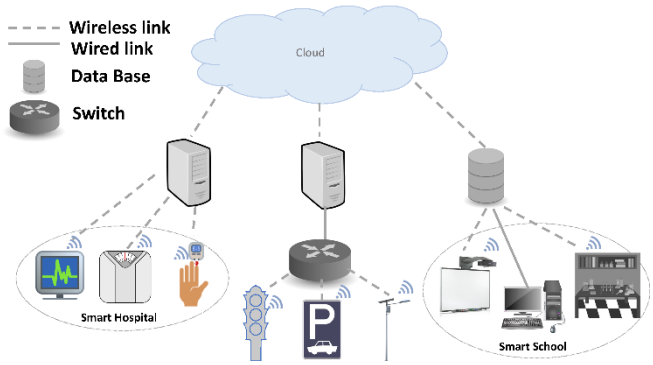

Figure 4. Hybrid: Tree star network topology

The mesh backbone ensures high connectivity and redundancy, while the tree-like subnetworks extend the network coverage to peripheral areas. This topology balances the benefits of the mesh structure with the scalability and cost-effectiveness of tree- like subnetworks. where this hierarchy often has three layers or more. Wide area networks frequently employ this structure [42].

5.2 Methodology

Network resilience is crucial for smart cities as it ensures the continuous operation of interconnected systems and services. A resilient network is quickly recovering from incidents like natural disasters, technical failures, or cyber-attacks.

In this research to measuring the network performance we apply different factors; we propose to measure the throughput of smart city network with the following parameters: Number of Nodes, type of attack, and type of network topology. We

have mainly considered graph centrality to determining their resilience coefficients for link failure, in the following analysis.

Graph centrality quantifies the relative importance of nodes within a network based on their structural position and connection patterns [43]. Various metrics capture different aspects of this importance, like direct connections, shortest paths, or information flow control. This paper explores the application of centrality measures in identifying critical links within smart city networks, with potential implications for both network optimization and vulnerability assessment. We have examined three different targeted attacks, namely (i) Degree (ii) Betweenness centrality (iii) CAA.

5.2.1 Betweenness centrality

Betweenness centrality quantifies the number of times a node acts as a bridge on the shortest path between two other nodes. A highly central node can significantly affect the flow of information in the network [43].

Can calculated by applying the following equation:
where, γ means the shortest path from one node X to another node Y, for a certain node n involved in the path.

5.2.2 Degree centrality

Degree centrality is based on the number of edges that connect to a node. It is often used to identify nodes that have the potential to quickly spread information due to their high number of connections [44].

5.3 Performance metrics

Evaluate the network resilient of smart city to determine the best network topology for smart city against three different kinds of targeted attacks as shown in Figure 5, in this paper, we propose to measure the resilience of smart city network in different types of typologies. First, we apply three different targeted attacks mentioned previously in the first type of topology which is the mesh topology, where apply each attack separately to get the influence of it in network. Then, we repeat the same previous steps in the other network topology which is the hybrid topology. where in section 6 we can see the effects of attacks on each topology. Finally, we decide the better network topology for smart city in case of a link failure through compare the result of each topology.

$$B_C = \sum_{X \neq Y \neq n} \frac{\gamma_{X,Y}(n)}{\gamma_{X,Y}} \quad (2)$$

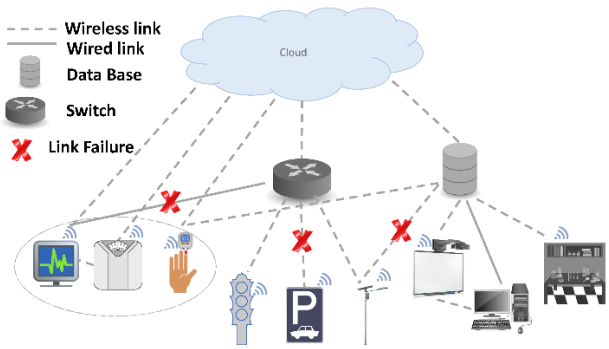

Figure 5. Network topology had a link failure attack

5.4 Experimental setup

All of our experiments were carried out on Windows, with 32 GB of RAM and a 1.80 GHz processor. Net- works were built using the Python library NetworkX, Anaconda Navigator (anaconda3), with application Scientific PYTHON Development Environment (Spyder) version (5.2.2). Spyder is a powerful integrated development environment for Python with advanced features for editing, interactive testing, debugging, and introspection.

6. RESULT AND DISCUSSION

In this section, the results of the proposed experiments will be presented and discussed. The performance of the proposed study was evaluated in terms of network resilience to attacks. I the course of the experiment, 50 nodes, 100 nodes, and 150 nodes were tested in each of the three types of targeted attack.

Our outcomes show that the (CAA) strategy is a good tool for understanding the resilience of smart city networks. By considering both BC and ND, CAA identifies critical links that may be observed by attacks focusing on just one centrality measure. This means that CAA can help network designers create more resilient networks by revealing vulnerabilities and showing decisions about network structure, backup connections, and defense strategies. CAA can also help network administrators and security professionals assess the resilience of existing networks by simulating attacks and identifying weak points that need extra protection.

Furthermore, CAA provides insights into effective defense strategies. By understanding the importance of betweenness centrality and node degree in different network scenarios, defenders can allocate resources and implement countermeasures accordingly. For example, in networks where global connectivity is crucial, defenders may prioritize protecting nodes with high betweenness centrality, while in networks where local connectivity is more important, defenders may focus on securing nodes with high degrees. This flexibility allows defenders to adapt their strategies based on the specific needs and characteristics of their smart city networks, ultimately enhancing the overall resilience against cyber threats.

6.1 Hybrid topology

In the first scenario, we applied the hybrid smart city topology. Figures 6(a)-6(c) show the charts for evaluation of the hybrid topology after three targeted attacks (Degree, Betweenness, and CAA) with 50, 100, and 150 nodes respectively. In Figure 6(a), we illustrate the effect of different targeted attacks on the largest connected components (network performance). It can be observed that after almost 40% of nodes were removed as a result of the attack, the network performance was reduced to 5% in the case of Degree and CAA targeted attacks. However, performance fell to 7% on removing only 20% of nodes in the case of the betweenness targeted attack. In Figure 6(b), it can be observed that after removing roughly 10% to 25% of nodes, the network performance was the best with the Degree targeted attack, while after removing about 30% of nodes all targeted attacks resulted in the same network performance. Moreover, after removing 40% of nodes, the performance of the network decayed to about 5%. In Figure 6(c), it is observed that after removing almost 33% of nodes the network performance decayed to about 3% for all types of targeted attacks. However, the performance of the network was better in the case of

Degree targeted attacks after removing 10% of nodes, while on removal of less than 10% of nodes all targeted attacks resulted in the same network performance. From Figures 6(a)-6(c) we detected that as the total number of nodes in the network increased, the performance of the network decayed with the lowest number of removed nodes. In most cases the Degree targeted attack was the most effective.

6.2 Mesh topology

In this scenario, we apply the mesh topology for the smart city in order to evaluate network performance through measuring the order of the largest connected component. Figures 7(a)-7(c) show the charts for evaluation of the mesh topology after applying the targeted attacks (Degree, Betweenness, and CAA), as previously mentioned, with 50,100, and 150 nodes respectively. In Figure 7(a), it is observed that after removing almost 50% of nodes as a result of different attacks, the network performance decayed to about 7% for Degree and CAA targeted attacks. However, the performance of the network was better in the case of Degree targeted attacks after removing 20% of nodes, while on removing less than 20% of nodes all targeted attacks.

6.3 Network resilience to different attack types

Network resilience is the ability o withstand potential changes. This study addressed three types of network attacks: CAA attacks, degree-based attacks, and betweenness-based attacks. Our results for all studied topologies and attacks have been summarized in in Table 3. We may note from this table, in general that mesh topology and a degree-based attack showed the highest network resilience in terms of the largest connected components (LCC), while hybrid topology with a betweenness- based attack showed the least network resilience.

From Table 3, it is clear that the network resilience in terms of the largest connected components is greatest in the case of a degree-based attack with the mesh topology network. In addition, the mesh network topology shows better network resilience with different attacks. The network resilience gives better results as the total number of nodes de- creases. Finally, it is detected that the network performance with betweenness-based and CAA attacks looks identical.

Based on the evaluation results, we can conclude that the mesh topology exhibits better network resilience compared to the hybrid topology under different targeted attack scenarios. The mesh topology, particularly with a degree-based attack, maintained the highest network performance in terms of the largest connected components. However, it is important to note that the resilience of both topologies is affected by the network size, with performance degrading when removing a lower percentage of nodes as the number of nodes increases, suggesting that scalability may impact the resilience of both topologies.

The mesh topology demonstrated some resilience against the CAA attack, with a slower performance decay when 15% to 50% of nodes were removed, while the degree-based attack had a more significant impact on the mesh topology as the network size increased. Overall, the mesh topology emerges as the more resilient option compared to the hybrid topology based on the evaluated scenarios.

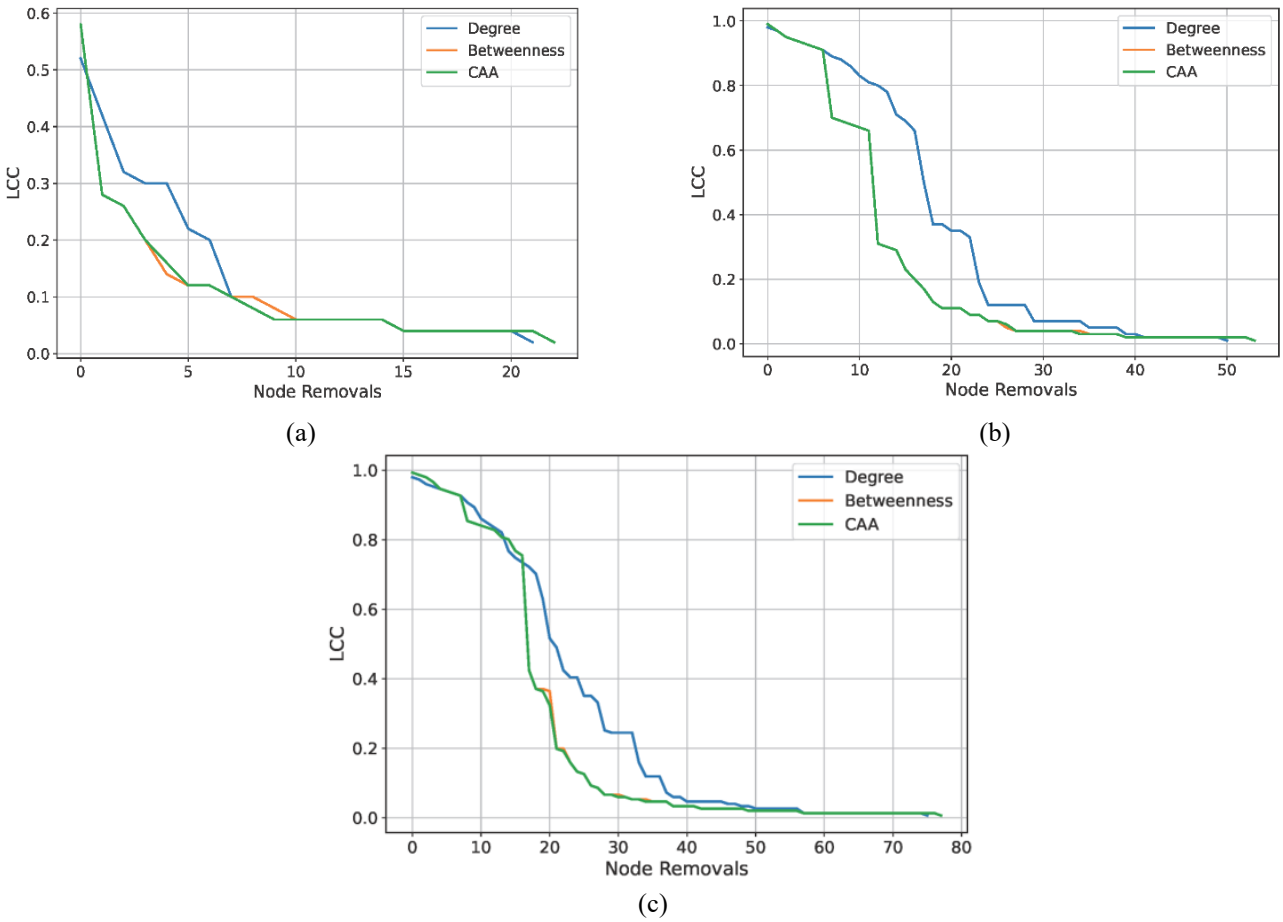

Figure 6. Evaluation of hybrid topology

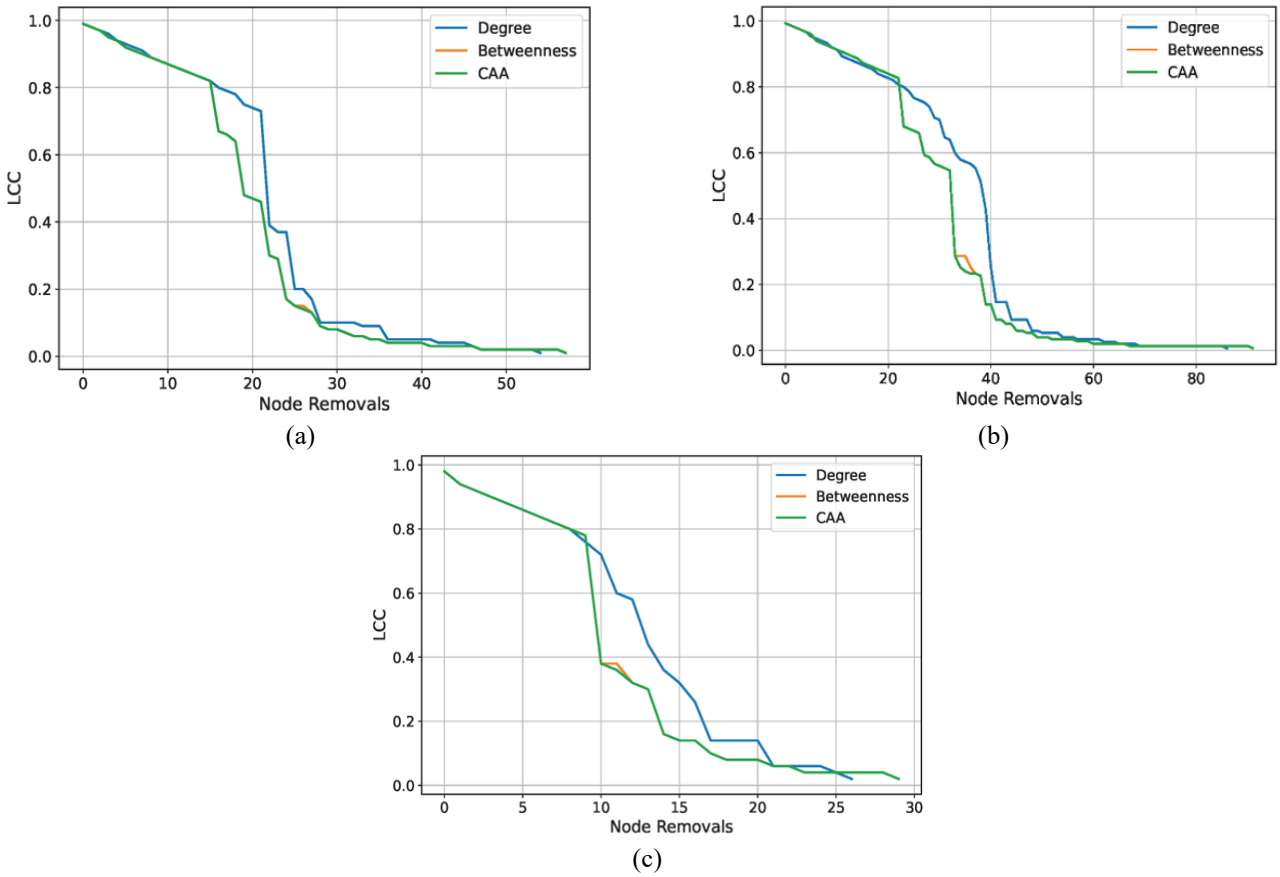

Figure 7. Evaluation the mesh topology

Table 3. The main aspect that differ between each topology

Aspect	Hybrid Topology	Mesh Topology
Network Resilience	Lower resilience compared to mesh topology	Higher network resilience compared to hybrid topology
Performance with Degree-based Attacks	Performs well in smaller networks but degrades rapidly as network size increases	Best performance among the evaluated scenarios
Performance with Betweenness-based Attacks	More vulnerable to betweenness-based attacks	Relatively more resilient compared to hybrid topology
Performance with CAA Attacks	Similar performance to betweenness-based attacks	shows some resilience, with slower performance decay when 15% to 50% of nodes are removed
Scalability	Suitable for smaller networks	Complexity increases with network size, affecting performance in larger networks
Resource Requirements	Requires fewer resources for implementation and maintenance	Higher cost and resource requirements for implementation and maintenance

Table 4. The evaluation result

Total Nodes	Removed Node	Hybrid Topology			Mesh Topology		
		BC	Degree	CAA	BC	Degree	CAA
50	5%	0.25	0.32	0.25	0.9	0.9	0.9
	10%	0.12	0.22	0.12	0.85	0.85	0.85
	20%	0.05	0.05	0.05	0.38	0.72	0.38
	30%	0.02	0.02	0.02	0.16	0.33	0.16
	40%	0.02	0.02	0.02	0.1	0.16	0.1
	50%	0.02	0.02	0.02	0.05	0.05	0.05
100	5%	0.9	0.9	0.9	0.9	0.91	0.9
	10%	0.66	0.82	0.66	0.86	0.86	0.86
	20%	0.12	0.37	0.12	0.45	0.75	0.45
	30%	0.05	0.1	0.05	0.09	0.12	0.09
	40%	0.02	0.03	0.02	0.08	0.09	0.08
	50%	0.02	0.02	0.02	0.02	0.02	0.02
150	5%	0.85	0.92	0.85	0.92	0.92	0.92
	10%	0.8	0.8	0.8	0.87	0.87	0.87
	20%	0.7	0.25	0.8	0.55	0.7	0.55
	30%	0.04	0.07	0.04	0.07	0.12	0.07
	40%	0.01	0.01	0.01	0.04	0.07	0.04
	50%	0.01	0.01	0.01	0.01	0.01	0.01

However, the choice of topology should also consider other factors such as scalability, cost, and specific network requirements. The mesh topology offers better resilience but comes with increased complexity and resource requirements, while the hybrid topology provides a balance between performance and complexity but may be more suitable for smaller networks. The insights gained from this study can guide the design and implementation of more resilient and secure smart city networks.

We figure out the mesh topology is more resilient than the hybrid topology. Also, the performance of the network between the three attacks is decreased slowly in the case.

Based on the comparison in the table, the mesh topology is more resilient against attacks compared to the hybrid topology. The Table 4 indicates that the mesh topology has higher network resilience overall and shows some resilience against CAA attacks, while the hybrid topology is more vulnerable to betweenness-based attacks.

From Table 3, it is clear that the network resilience in terms of the largest connected components is greatest in the case of a degree-based attack with the mesh topology network. In addition, the mesh network topology shows better network resilience with different attacks. The network resilience gives better results as the total number of nodes de- creases. Finally, the analysis indicates that the network performance under betweenness-based, and CAA attacks demonstrates comparable behavior.

7. CONCLUSIONS AND FUTURE WORK

In this study, we have investigated the resilience of smart city network topologies against targeted attacks using centrality-based strategies. We proposed a novel Centrality Adaptive Attack (CAA) strategy that considers both the betweenness centrality and node degree of network nodes to identify critical links for targeted attacks. Through extensive experiments on generated mesh and hybrid network topologies, we demonstrated the effectiveness of the CAA strategy in disrupting network connectivity and performance com- pared to random and other centrality-based attack strategies.

We figure out the mesh topology is more resilient than the hybrid topology. Also, the performance of the network between the three attacks is decreased slowly in the case of CAA rather than the other attacks, where its removed node between 15% to 50% of nodes, while the network performance reduced in faster rate with targeted degree- based link attack. Otherwise, we highlight the importance of considering multiple centrality measures when assessing the resilience of smart city networks against targeted attacks. The CAA strategy provides a more comprehensive approach to identifying critical links and can help network designers and operators to develop more robust and resilient network architectures. By understanding the vulnerabilities of different network topologies and the impact of targeted attacks, smart city planners can make informed decisions about network design, redundancy, and security measures.

However, it is important to acknowledge that our current study reliesa on generated network topologies and does not use real-world smart city network data. While the generated topologies are based on common structures and properties observed in smart city networks, they may not fully capture the complexity and heterogeneity of actual deployments. Therefore, validating our findings using real-world data is a crucial next step in assessing the applicability of our results to practical scenarios.

Based on our evaluation results, we provide the following practical guidelines for network designers to enhance the resilience of smart city networks against targeted attacks:

- Identify critical nodes: Use the CAA algorithm to identify nodes with high betweenness centrality and node degree. Prioritize these critical nodes in topology design and ensure they have redundant connections and protection against failures or attacks.
- Enhance redundancy: Incorporate redundant paths and connections in the network topology to improve resilience. Provide multiple routes between nodes and ensure alternative paths are available for data transmission.
- Mesh and hybrid topologies: Consider implementing mesh or hybrid network topologies in smart city networks based on our findings. Mesh and hybrid topologies can provide increased resilience, flexibility, and coverage compared to traditional hierarchical or centralized architectures.
- Balance centrality and distribution: Achieving a balance between centralized and distributed network architectures. Finding the optimal balance based on the requirements and constraints of the smart city network, while considering the balance between control, flexibility, and complexity.
- Monitor and update regularly: Continuously monitor the network topology and performance using the CAA algorithm or other network analysis tools. Adapt and update the topology based on the insights gained from monitoring and analysis to identify vulnerabilities and assess the effectiveness of resilience strategies.

7.1 Future work

There are several promising directions for future re- search based on the findings and limitations of our current study. Firstly, as mentioned in the conclusion, validating our results using real- world smart city network data is a top priority. By collaborating with smart city operators and obtaining access to actual network topology and traffic data, we can assess the effectiveness of the CAA strategy and other centrality-based attacks in realistic settings. This will help to identify any additional factors or constraints that may influence the resilience of smart city networks and refine our attack models accordingly.

Secondly, our current study focuses on the structural resilience of network topologies and does not take into account the impact of the network's dynamic adaptation or recovery mechanisms. In real-world smart city networks, various resilience strategies such as traffic rerouting, backup paths, and self- healing mechanisms may be employed to mitigate the im- pact of attacks. Investigating the interplay between targeted attacks and these resilience strategies is an important avenue for future research. By modeling and simulating dynamic network behavior, we can gain a more comprehensive understanding of the resilience of smart city networks and develop more effective defence mechanisms.

Thirdly, the CAA strategy can be further enhanced by incorporating additional centrality measures or network properties. For example, considering the closeness centrality or the clustering coefficient of nodes may provide additional in- sights into the criticality of network components. Exploring the combination of different centrality measures and their

relative importance in various smart city network scenarios can lead to more sophisticated and targeted attack strategies. Lastly, our study can be extended to investigate the resilience of other types of complex networks, such as transportation networks, power grids, and social networks. By applying the CAA strategy and other centrality-based attacks to these networks, we can identify common vulnerabilities and develop generalized resilience frameworks. Comparative studies across different network domains can provide valuable insights into the universality and transferability of our findings.

For future research will validate our findings with real-world data and expand the evaluation of network resilience elsewhere the (LCC). This will involve incorporating additional metrics such as flow robustness, connectivity, assortativity, edge boundary, and redundancy to capture a broader range of network performance and resilience aspects. This multi-faceted approach will provide a more comprehensive understanding of resilience and informing the design of robust infrastructure for smart cities.

ACKNOWLEDGMENT

The authors extend their appreciation to Researcher Supporting Project number (RSPD2025R582), King Saud University, Riyadh, Saudi Arabia.

REFERENCES

[1] Unesco cities platform. https://shorturl.at/enwy3, 2020.

[2] Buettner, T. (2015). Urban estimates and projections at the United Nations: The strengths, weaknesses, and underpinnings of the world urbanization prospects. Spatial Demography, 3(2): 91-108. https://doi.org/10.1007/s40980-015-0004-2

[3] Arasteh, H., Hosseinnezhad, V., Loia, V., Tommasetti, A., Troisi, O., Shafie-Khah, M., Siano, P. (2016). IoT-based smart cities: A survey. In 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), Florence, Italy, pp. 1-6. https://doi.org/10.1109/EEEIC.2016.7555867

[4] Peris-Ortiz, M., Bennett, D.R., Yábar, D.P.B. (2016). Sustainable smart cities: Creating spaces for technological, social and business development. Boletín Científico de las Ciencias Económico Administrativas del ICEA, XIV, 224. https://doi.org/10.1007/978-3-319-40895-8

[5] Mehmood, Y., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M., Guizani, S. (2017). Internet-of-things-based smart cities: Recent advances and challenges. IEEE Communications Magazine, 55(9): 16-24. https://doi.org/10.1109/MCOM.2017.1600514

[6] Bao, L., Garcia-Luna-Aceves, J.J. (2003). Topology management in ad hoc networks. In Proceedings of the 4th ACM International Symposium on Mobile ad Hoc Networking & Computing, pp. 129-140. https://doi.org/10.1145/778415.778432

[7] Alderson, D., Li, L., Willinger, W., Doyle, J.C. (2005). Understanding internet topology: Principles, models, and validation. IEEE/ACM Transactions on Networking, 13(6): 1205-1218. https://doi.org/10.1109/TNET.2005.861250

[8] Hossain, M.M., Fotouhi, M., Hasan, R. (2015). Towards an analysis of security issues, challenges, and open problems in the internet of things. In 2015 IEEE World Congress on Services, New York, NY, USA, pp. 21-28. https://doi.org/10.1109/SERVICES.2015.12

[9] Sharma, P., Jain, S., Gupta, S., Chamola, V. (2021). Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. Ad Hoc Networks, 123: 102685. https://doi.org/10.1016/j.adhoc.2021.102685

[10] Jawhar, I., Mohamed, N., Al-Jaroodi, J. (2018). Networking architectures and protocols for smart city systems. Journal of Internet Services and Applications, 9(1): 26. https://doi.org/10.1186/s13174-018-0097-0

[11] Meng, F., Fu, G., Farmani, R., Sweetapple, C., Butler, D. (2018). Topological attributes of network resilience: A study in water distribution systems. Water Research, 143: 376-386. https://doi.org/10.1016/j.watres.2018.06.048

[12] Alenazi, M.J. (2015). Network resilience improvement and evaluation using link additions. PhD thesis, University of Kansas.

[13] Guns, R., Liu, Y.X., Mahbuba, D. (2011). Q-measures and betweenness centrality in a collaboration network: A case study of the field of informetrics. Scientometrics, 87(1): 133-147. https://doi.org/10.1007/s11192-010-0332-3

[14] Cui, L., Xie, G., Qu, Y., Gao, L., Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. IEEE Access, 6: 46134-46145. https://doi.org/10.1109/ACCESS.2018.2853985

[15] Modarresi, A., Sterbenz, J.P. (2017). Multilevel IoT model for smart cities resilience. In Proceedings of the 12th International Conference on Future Internet Technologies, pp. 1-7. https://doi.org/10.1145/3095786.3095793

[16] Cholda, P., Mykkeltveit, A., Helvik, B.E., Wittner, O.J., Jajszczyk, A. (2007). A survey of resilience differentiation frameworks in communication networks. IEEE Communications Surveys & Tutorials, 9(4): 32-55.

[17] Smith, P., Hutchison, D., Sterbenz, J.P., Schöller, M., Fessi, A., Karaliopoulos, M., Plattner, B. (2011). Network resilience: A systematic approach. IEEE Communications Magazine, 49(7): 88-97. https://doi.org/10.1109/MCOM.2011.5936160

[18] Amiri, Z., Heidari, A., Navimipour, N.J., Unal, M. (2023). Resilient and dependability management in distributed environments: A systematic and comprehensive literature review. Cluster Computing, 26(2): 1565-1600. https://doi.org/10.1007/s10586-022-03738-5

[19] Kreutz, D., Ramos, F.M., Verissimo, P.E., Rothenberg, C.E., Azodolmolky, S., Uhlig, S. (2014). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1): 14-76. https://doi.org/10.1109/JPROC.2014.2371999

[20] Tornatore, M., André, J., Babarczi, P., Braun, T., Følstad, E., Heegaard, P., Voyiatzis, A. (2016). A survey on network resiliency methodologies against weather-based disruptions. In 2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM), Halmstad, Sweden, pp. 23-34. https://doi.org/10.1109/RNDM.2016.7608264

[21] Aljohani, S.L., Alenazi, M.J. (2021). MPResiSDN: Multipath resilient routing scheme for SDN-enabled smart cities networks. Applied Sciences, 11(4): 1900.

https://doi.org/10.3390/app11041900
[22] Zhou, Q., Zhu, M., Qiao, Y., Zhang, X., Chen, J. (2021). Achieving resilience through smart cities? Evidence from China. Habitat International, 111: 102348. https://doi.org/10.1016/j.habitatint.2021.102348
[23] Das, L., Munikoti, S., Natarajan, B., Srinivasan, B. (2020). Measuring smart grid resilience: Methods, challenges and opportunities. Renewable and Sustainable Energy Reviews, 130: 109918. https://doi.org/10.1016/j.rser.2020.109918
[24] Samarakkody, A., Amaratunga, D., Haigh, R. (2022). Characterising smartness to make smart cities resilient. Sustainability, 14(19): 12716. https://doi.org/10.3390/su141912716
[25] Syed, A.S., Sierra-Sosa, D., Kumar, A., Elmaghraby, A. (2021). IoT in smart cities: A survey of technologies, practices and challenges. Smart Cities, 4(2): 429-475. https://doi.org/10.3390/smartcities4020024
[26] Estrada, E. (2006). Network robustness to targeted attacks. The interplay of expansibility and degree distribution. The European Physical Journal B-Condensed Matter and Complex Systems, 52: 563-574. https://doi.org/10.1140/epjb/e2006-00330-7
[27] Al-Zoman, R., Alenazi, M.J. (2020). Exploiting SDN to improve QoS of smart city networks against link failures. In 2020 Seventh International Conference on Software Defined Systems (SDS), Paris, France, pp. 100-106. https://doi.org/10.1109/SDS49854.2020.9143878
[28] Alenazi, M.J., Cetinkaya, E.K. (2020). Resilient placement of SDN controllers exploiting disjoint paths. Transactions on Emerging Telecommunications Technologies, 31(2): e3725. https://doi.org/10.1002/ett.3725
[29] Alablani, I., Alenazi, M. (2020). EDTD-SC: An IoT sensor deployment strategy for smart cities. Sensors, 20(24): 7191. https://doi.org/10.3390/s20247191
[30] Ibrahim, A.S., Youssef, K.Y., Eldeeb, A.H., Abouelatta, M., Kamel, H. (2022). Adaptive aggregation based IoT traffic patterns for optimizing smart city network performance. Alexandria Engineering Journal, 61(12): 9553-9568. https://doi.org/10.1016/j.aej.2022.03.037
[31] Marksteiner, S., Jimenez, V.J.E., Valiant, H., Zeiner, H. (2017). An overview of wireless IoT protocol security in the smart home domain. 2017 Internet of Things Business Models, Users, and Networks, Copenhagen, Denmark, pp. 1-8. https://doi.org/10.1109/CTTE.2017.8260940
[32] Piraveenan, M., Uddin, S., Chung, K.S.K. (2012). Measuring topological robustness of networks under sustained targeted attacks. In 2012 IEEE/ACM international conference on advances in social networks analysis and mining, pp. 38-45. https://doi.org/10.1109/ASONAM.2012.17
[33] Huang, X. (2020). Multi-node topology location model of smart city based on Internet of Things. Computer Communications, 152: 282-295. https://doi.org/10.1016/j.comcom.2020.01.052
[34] Bhandari, K.S., Cho, G.H. (2020). Resource oriented topology construction to ensure high reliability in IoT based smart city networks. International Journal of System Assurance Engineering and Management, 11(4): 798-805. https://doi.org/10.1007/s13198-019-00861-2
[35] Pasolini, G., Buratti, C., Feltrin, L., Zabini, F., De Castro, C., Verdone, R., Andrisano, O. (2018). Smart city pilot projects using LoRa and IEEE802. 15.4 technologies. Sensors, 18(4): 1118. https://doi.org/10.3390/s18041118
[36] Brandes, U. (2001). A faster algorithm for betweenness centrality. Journal of Mathematical Sociology, 25(2): 163-177. https://doi.org/10.1080/0022250X.2001.9990249
[37] Xin, R.S., Gonzalez, J.E., Franklin, M.J., Stoica, I. (2013). Graphx: A resilient distributed graph system on spark. In First International Workshop on Graph Data Management Experiences and Systems, pp. 1-6. https://doi.org/10.1145/2484425.2484427
[38] Riondato, M., Kornaropoulos, E.M. (2014). Fast approximation of betweenness centrality through sampling. In Proceedings of the 7th ACM International Conference on Web Search and Data Mining, pp. 413-422. https://doi.org/10.1145/2556195.255622
[39] Geisberger, R., Sanders, P., Schultes, D. (2008). Better approximation of betweenness centrality. In 2008 Proceedings of the Tenth Workshop on Algorithm Engineering and Experiments (ALENEX), pp. 90-100. https://doi.org/10.1137/1.9781611972887.9
[40] AlGhamdi, Z., Jamour, F., Skiadopoulos, S., Kalnis, P. (2017). A benchmark for betweenness centrality approximation algorithms on large graphs. In Proceedings of the 29th International Conference on Scientific and Statistical Database Management, pp. 1-12. https://doi.org/10.1145/3085504.3085510
[41] Bahmani, B., Chowdhury, A., Goel, A. (2010). Fast incremental and personalized pagerank. arXiv preprint arXiv:1006.2880. https://doi.org/10.48550/arXiv.1006.2880
[42] Musa, A. (2020). A proposet network topology for low cost scenarios in a large scale network within a smart city. PhD thesis, Universidade Federal de Alagoas.
[43] Camacho, D., Panizo-LLedot, A., Bello-Orgaz, G., Gonzalez-Pardo, A., Cambria, E. (2020). The four dimensions of social network analysis: An overview of research methods, applications, and software tools. Information Fusion, 63: 88-120. https://doi.org/10.1016/j.inffus.2020.05.009
[44] Yao, Q., Li, R.Y.M., Song, L., Crabbe, M.J.C. (2021). Construction safety knowledge sharing on Twitter: A social network analysis. Safety Science, 143: 105411. https://doi.org/10.1016/j.ssci.2021.105411