Received: 2026-05-14
Accepted: 2026-07-15
Published Online: 2026-07-20
DOI: 10.70454/JRICST.2026.030303

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

Location Hiding Architecture for Mitigating DDoS Attacks in SCADA Systems

Dr. Deepak kumar*[1], Raj Kamal [2]

[1]Professor, College of Science & Technology, Surajmal University, Uttrakhnad, India
[2]Assistant Professor, Department of CSE, Surajmal University,Uttrakhnad, India

***Corresponding Author:** deepakraj.377@gmail.com

This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

Distributed Denial of Service (DDoS) attacks are posing an increasing threat to SCADA systems, which are the core infrastructure for power grids, water treatment, oil and gas pipelines, and many other critical infrastructure systems. The growing connectivity of such systems and their dependence on legacy communication protocols make them quite susceptible to large-scale disruptions. This paper introduces a novel Location Hiding Architecture (LHA) for the protection of SCADA systems to improve the security and availability by hiding the real network location of the interested entity. The proposed architecture employs a multi-layer proxy mechanism with two types of proxies - setup and data. The system design keeps the public access interface separate from the SCADA core and ensures that an attacker can never directly see critical assets, much less target them. With dynamic proxy allocation, hidden routing paths, and anycast-based proxy distribution, we achieve scalability, resilience, and fast removal of compromised nodes from the system. Furthermore, it has adaptive traffic filtering and controlled access for reducing bad interactions. Simulation results show that a proxy density of 0. 5% can successfully block more than 93% of the DDoS traffic even when malicious nodes constitute as much as 10% of the network. The presented LHA framework enables a strong, scalable, defensive layer to effectively secure modern SCADA against evolving cyber threats.

Keywords: Cyber-Attack, Distributed Denial of Service, SCADA, Protection.

1.0 Introduction

SCADA is employed to manage critical infrastructure such as electricity, water, and oil pipelines. As these systems are network-connected and frequently use outdated technology, they are susceptible to being overwhelmed by DDoS attacks, which can effectively prevent them from operating [1]. Location Hiding Architecture (LHA) is a means to secure SCADA. The real location (IP address) of our critical servers are hidden so attackers cannot locate or attack them directly. It achieves this by isolating the public network from the true SCADA system, thereby keeping the real system safe and hidden [2]. A distributed denial-of-service (DDoS) attack is a method of flooding a particular service with so many concurrent requests to overburden that service. Distributed denial of service attack aims to make an online service unavailable by overwhelming it with traffic from multiple sources. Another popular cheat attack is sending broken packates, which can crash or reboot victim's PC by exploiting applications or protocols used by adorers. DDoS attacks are not based on any particular network protocol or system vulnerability, but Rather attack the Internet and its networked victim Access to

Received: 2026-05-14
Accepted: 2026-07-15
Published Online: 2026-07-20
DOI: 10.70454/JRICST.2026.030303

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

find incident sources. Using the easy availability of the Internet to locate targets and distribute malicious code, the attacker. The hacker then establishes an attack infrastructure by communicating with masters that orders bots [3].

In 2020 [4,] the Internet was vulnerable to Distributed Denial of Service attacks because it was relied on for too many things. predicts over 15 million DDoS attacks in 2023, increasing from 7.9 million in 2018 [4][7]. Location Hiding Architecture is a defense mechanism that shields the critical components of SCADA systems from DDoS attacks while hiding their actual network address behind a network of proxies, relay nodes, and secure communication layers.

2.0 Related Work

Many businesses rely on SCADA systems to run their operations. Cyberattacks, particularly distributed denial of service attacks, are becoming more common. A distributed denial of service (DDoS) attack aims to flood a target with so much traffic that its intended audience is unable to access it. SCADA infrastructure is seriously at risk from DDoS attacks [5][6]. Nonetheless, severaldefences can be put in place to lessen the likelihood of an attack. Securing SCADA systems is crucial due to the potentially disastrous consequences of a successful DDoS assault. SCADA system security must be a primary concern to prevent economic, environmental, and public safety disasters from interfering with vital infrastructure and industrial processes [8] [13].

The existing literature has highlighted several methodologies for the detection and mitigation of DDoS attacks in SCADA, SDN and IIoT environments. A multi-model proposal for classification and detection of DDoS attacks on SCADA systems proposes a multi-model technique to improve the detection accuracy of SCADA systems and CIDS: A collaborative intrusion detection system approach for SDN-based distributed industrial plants [9] [10]. The authors propose a collaborative IDS framework for distributed industrial networks. Similarly, security of high altitude platform stations: Threat Taxonomy, Attacks and Defences with Standards Mapping DDoS Attack Use Case Provides a comprehensive taxonomy of DDoS threats and defence mechanisms. Top 5 most famous DDoS attacks: Real-world insights Top 5 most famous DDoS attacks covers the impact of DDoS attacks. Moreover, AI-based cybersecurity for SCADA-integrated microgrids: The real-time detection framework proposes an AI-based real-time detection model [11] [12].

2.1 Problem

To interfere with the victim's service availability, DDoS attacks might employ a variety of attack sources, packet-transmission techniques, and packet formats. Defence systems must use a variety of DDoS detection methods to lessen the impact of DDoS attacks. This might be too slow to be useful for making improvements in real time, depending on the computational operations required. The DoS management architecture includes security coverage prior to, during, and following an incident. To achieve this, we offer a thorough plan and specific suggestions for enhancing the technical and operational aspects of:

• Protection against DoS attacks is crucial.

• The capacity to recognise attacks as they occur.

2.2 Contributions

In order to conceal the destination from the source and intermediary nodes, we present a feasible architecture that provides a source destination using many IP addresses, none of which are the destination's actual IP address. Additionally, this design uses anycast SPs to protect against

Received: 2026-05-14
Accepted: 2026-07-15
Published Online: 2026-07-20
DOI: 10.70454/JRICST.2026.030303

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

distributed denial of service attacks. Additionally, it is safer (and better) to locate proxies since the architecture disperses (and dilutes) possible attackers. Attackers can be restricted to smaller areas with anycast SPs, which makes it easier to find them or solve client challenges. By employing this paradigm, the service can gradually deteriorate by releasing data proxies to its authorised users based on their reliability without interfering with its availability or creating inconsistent user experiences.Complete hiding of destination networks is accomplished by using the multicast routing mechanisms of current routers; secret pathways can be built and dynamically formed or removed as needed.

2.3 Difficulties in Hiding Location

For location-hiding architectures, the destination should be hidden even in the case of compromised or malicious proxies. Important factors to consider are decreasing the number of trusted components, controlling the information released to the proxies, and controlling the path of the proxies to the location of the service. The attacker can skip the proxy and go straight to their intended victim if they already know the target's address. These threats can be mitigated by creating a protective filtering perimeter around the destination that reduces the amount of malicious traffic that can reach the destination, even if the destination address is compromised. But filtering has its own challenges, for instance, the requirement of a large enough filtering perimeter to cater for bottlenecks close to the destination network [14].

For location-hiding architectures to be effective, the service must be resilient to attacks on the proxies. Now, the attacker will attack the proxies and not the original target [15]. One way to counter attacks against the proxies is to use a large number of proxies and to change them frequently. However, proxies should be lightweight, so that they can be recruited in large numbers, and deployed quickly - this means not requiring any specialised hardware or software, and not storing any private user data. A way to obtain a large number of proxies is by recruiting them from end hosts, for example, those in P2P networks.

Location-hiding architectures are responsible for assigning and managing proxies in a manner that minimises the risk to legitimate users. Increasing the number of proxies can make the target more diffuse, but a single proxy attack can still affect a legitimate client. The attacker may attack certain proxies in order to disable or otherwise disrupt certain parts of the proxy network. In the face of massive DDoS attacks, the destination must allocate and manage proxies to protect legitimate users as much as possible.

Finally, a scalable and reliable discovery mechanism is needed for clients to learn about the proxies in location-hiding architectures. Discovery mechanism enables clients to discover the proxies they need to access the service. However, the discovery service must be attack-resilient and able to cope with frequent changes in the proxy set, otherwise it becomes a single point of failure for the whole system in a short time.

2.4 DDoS Attack and Flash Crowd

A distributed denial of service (DDoS) attack or flash crowd can cause a large spike in traffic to a website or service. Rather than a coordinated attack to overload and disrupt the target's online services as in a distributed denial of service (DDoS) attack, a flash crowd is a sudden and temporary surge in legitimate user traffic brought about by the interest of actual users. Regarding what causes them, what they are used for, how long they last and what preparations should be made in advance, these two phenomena could not be more different. But DDoS attacks have special defense needs to separate out the bad traffic, so the infrastructure needs a temporary boost to deal with the genuine interest of a flash crowd. Our work is motivated by the contrast between flash crowds and DDoS attack traffic volume behavior. Hence, the resemblance between flash crowd flow and DDoS attacks

Received: 2026-05-14
Accepted: 2026-07-15
Published Online: 2026-07-20
DOI: 10.70454/JRICST.2026.030303

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

are incomparable. Resemblances between DDoS attack and flash mob force one to make a clear distinction between the two to avoid false alarms. It's hard to tell the distributed-denial-of-service flooding attacks from flash events, and defenders get the worst of that. We're going to have a horrible time if we couldn't make it happen. On the one hand, opponents can deceive our detectors by simulating flash crowd traffic profiles. However, our sensors may confuse spontaneous flash mobs with destructive DDoS attacks.

3.0 ARCHITECTURES FOR HIDING LOCATION

Architectures for hiding location are systems designed to protect a user's real geographic position while they access services.

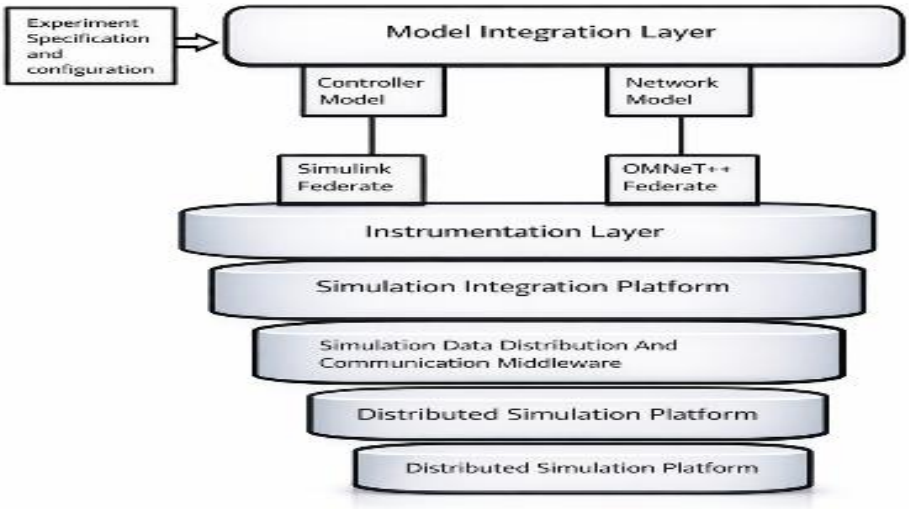

Fig. 1: Tentative Simulation Architecture

Figure 1 shows a layered architecture to run complex simulations by combining different models and systems. The experiment is characterized at the top by a choice of configurations and parameters. In the model integration layer, different types of models are linked, e.g. controller models (decision-making) and network models (communication) via tools like Simulink and OMNeT++. Underneath this, the instrumentation layer observes the simulation and collects vital data. The simulation integration platform ensures the coordination of all the parts of the system, in particular in terms of timing and interaction. Further down the data distribution and communication middleware takes care of the exchange of information between components, which is especially relevant if simulations are executed on multiple machines. Finally, the distributed simulation platform simulates the

Location-hiding services such as Architecture and The Onion Router hide the IP address of the final destination and limit access to the service through intermediaries. These architectures uses large amount of proxies to pretend some level of power and provide changing configurations of working proxies to confuse attackers. In contrast to the Onion Router which provides location hidden services using an overlay based anonymisation network, this architecture uses the underlying network to hide the service and is not anonymity enabled. Overlay nodes, colloquially termed "introduction points", permit a hidden destination on the Onion Router to establish encrypted connections with other destinations. This Onion Router's own service is available to be dialed by any service-requestor who wants to obtain a list of entry points. Then it chooses one of the entry points and makes a connection to the final hop through a third node, a rendezvous point in The Onion Router. There is no one knows

Received: 2026-05-14
Accepted: 2026-07-15
Published Online: 2026-07-20
DOI: 10.70454/JRICST.2026.030303

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

the other person's IP address in this scenario. The first node of The Onion Router, its initial node also symbolize the architecture's settings and its information respectively for refer to. Architecture is immune to this type of attack, as its backdoors always originate at the core routers of the network.

Valet Service also suggests additional introduction points to be wrapped in a maze of valet nodes. At first, users connected to a centralized, direct The Onion Router service to get information about which proxies were available. A Distributed Denial of Service (DDoS) attack can be mounted against the Onion Router service. The design uses Domain Name System (DNS) to find available proxies, but it safeguards the discovery service with traditional countermeasures against DNS attacks. By building an overlay of proxies and assigning certain proxies to hold different types of information about the overlay and the destination, Mayday is essentially a generalized form of Secure Overlay Services (SOS). A proxy can be used by anyone, but traffic is routed through that proxy only for authenticated users. To defend the target, SOS establishes a buffer that allows only data packets to flow in from the hidden servlets.

Location-hiding designs such as Architecture and SOS run into the unique challenge of how to efficiently distribute authentication information to all proxies. Their integration is enabled by the multitenancy nature of architecture proxies characterized by small size and no dependence on an individual user's credentials. To defend SP patrons against DP-level compromises, they run a cluster of proxies. Since the attacker cannot tell which DP the client is using, a service-level assault will cause less collateral damage among unsuspecting users as well. Clients have an easy way out if a proxy is compromised: they can switch to a different one, in SOS's case. Due to proxy failures, Architecture clients may experience intermittent services interruption. Internet Indirection Infrastructure (i3) is a novel system that redefines the mapping of IP addresses to physical locations by building an overlay on the existing Internet. The client locates the service's unique ID, and then sends a request to that ID. The request is executed at its last stage, via the underlying i3 overlay, and the final destination may return a fresh batch of private IDs to the requesting client. Penetration attacks, reconfiguration, proxy depth, and host diversity are challenges that all overlay-based location-hiding systems such as SOS, i3, and The Onion Router have to contend with. Because it is dependent on the routers of the underlying network, the security of the architecture can only be as strong as the routers. Network authenticated path panning (SNAPP) maintains anonymous senders without regard for routing protocol decisions. Proxy servers offer an effective means of safeguarding SCADA systems against DDoS attacks.

The proposed Location Hiding Architecture (LHA) is modeled as a network graph G = (V, E), where V comprises clients, proxy nodes, and hidden SCADA servers, and E represents communication links. Let C, P = P_s ∪P_d, and S denote the sets of clients, proxies (setup and data), and servers, respectively. The aggregate traffic at a proxy $p \in P$ is expressed as $T_p = \Sigma_{c\in C} \lambda_c + \Sigma_{a\in A} \lambda_a$, where λ_c and λ_a denote legitimate and malicious traffic rates. Each proxy operates under a capacity constraint μ_p, and service degradation occurs when $T_p>\mu_p$. The filtering mechanism attenuates malicious traffic by a factor α, yielding an effective attack rate $\lambda_a^{eff} = (1 - \alpha)\lambda_a$. The probability of target exposure is inversely proportional to the number of data proxies, i.e., $P_{discover} = 1/|P_d|$, thereby enhancing location anonymity with increased proxy diversity. The system availability is defined as $A_v = 1 - (\lambda_a^{eff} / (\lambda_c + \lambda_a))$, indicating improved resilience with higher filtering efficiency. Furthermore, mitigation effectiveness scales with the proxy density $\rho = |P|/|V|$, supporting robust and scalable defenses against DDoS attacks in SCADA environments.

Received: 2026-05-14
Accepted: 2026-07-15
Published Online: 2026-07-20
DOI: 10.70454/JRICST.2026.030303

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

3.1 Identifying Misbehaving Proxies

If the proxy tries to overwhelm the destination with these fake report messages, D will be aware of it and disconnect the proxy. D, for instance, might decide on a maximum allowable path length. If D receives more than this threshold number of report messages, it will disconnect from the proxy. That is, if multiple routers have identical prefixes (for example, a /16 and a /24), the first router with the largest matching prefix is chosen as the proxy.

4.0 Results and Discussion

We show the effectiveness of anycast SPs through simulations on an Internet-scale architecture. Our research indicates that even when malicious users occupy 10% of the network, an SP density of 0.5% is sufficient to suppress more than 93% of the attackers. Even at a density of just 0.01% of authentic clients, this remains true. Furthermore, at that density, just one attacker is often interfering with genuine clients at a particular SP, and attackers are limited to an area no more than three or four hops from the SPs.

Dynamic location-hiding architectures can significantly increase the security of SCADA systems against DDoS attacks. Protect SCADA systems by making them more challenging by continuously changing their IP addresses.

We prove the following by constructing a miniature test of architectural design:

1) By turning off route announcements for the destination network into the global Internet, the destination network can be kept completely hidden.

2) Present-day routers' support for multicast routing enables the creation of covert routes. For this goal, we can employ Single Source Multicast.

3) it only takes a few seconds, tops, to add or remove a hidden path. As a result, it would be simple to add new proxies and swiftly remove compromised proxies once they are discovered.

5.0 Conclusion

Since the invention of the Internet, many services that were once only offered in person have moved to the virtual world. This includes the economic and energetic markets, political, diplomatic, and military arenas. DDoS (distributed denial of service) attacks, however, challenge the security and reliability of these services. As a countermeasure to a new form of distributed denial of service attacks, the location-hiding architecture is proposed in this status report. Since neither the proxies nor the origin know the destination IP address, this furthers the location-hiding property. For security reasons, there is no way to ping from the outside to inside; or from inside to outside, you just cannot access the hosts directly. Data proxies remain secret unless requested by an authorized user but setup proxies are available to anyone who needs them. Without knowing the specific data proxy used by a particular client first, the attacker can't attack the live communications between real clients in the network. The use of IP anycast within the architecture also helps identify the source of any abuse. The attacker has the opportunity to build large botnet since the setup proxies can be obtained easily. The setup proxies enable any part of the architecture to get permission from the target system. The destination can disable the concealed path to thwart an assault if the attacker is within three or four hops of the SPs. The effectiveness of the architecture is demonstrated by simulations on an Internet-scale network topology, which reveal that a sparse SP density of 0.5% is adequate to suppress over 93% of attackers even when just 10% of the network is occupied. The design allows the endpoint to choose its own recipient lists and proxy assignment process.

Received: 2026-05-14
Accepted: 2026-07-15
Published Online: 2026-07-20
DOI: 10.70454/JRICST.2026.030303

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

Author Contributions

All of the writers agreed on the study's substance. The author has reviewed and approved the final manuscript.

Funding

The authors did not receive any specific funding for this work.

Conflicts of Interest

The authors declare no conflicts of interest.

Reference

[1] E. Söğüt and O. A. Erdem, "A multi-model proposal for classification and detection of DDoS attacks on SCADA systems," Applied Sciences, vol. 13, no. 10, p. 5993, 2023, doi: 10.3390/app13105993.

[2] F. Alenezi, S. Almowuena, A. Alenezi, and M. J. F. Alenazi, "CIDS: A collaborative intrusion detection system approach for SDN-based distributed industrial plants," Transactions on Emerging Telecommunications Technologies, vol. 37, no. 1, p. e70327, 2026, doi: 10.1002/ett.70327.

[3] C. Hjaiji, B. Ouni, and M.-S. Alouini, "Cybersecurity of high-altitude platform stations: Threat taxonomy, attacks and defenses with standards mapping—DDoS attack use case," IEEE Open Journal of the Communications Society, vol. 7, pp. 328–352, 2026, doi: 10.1109/OJCOMS.2025.3650132.

[4] Microsoft 365, "Top 5 most famous DDoS attacks," Feb. 17, 2023. [Online]. Available: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/top-5-most-famous-ddos-attacks

[5] A. S. Athamnih et al., "AI-driven cybersecurity for SCADA-integrated microgrids: A real-time detection framework," in Proc. IEEE 5th Int. Conf. AI in Cybersecurity (ICAIC), Houston, TX, USA, 2026, pp. 1–6, doi: 10.1109/ICAIC67076.2026.11395662.

[6] M. Hassan, A. Gumaei, S. Huda, and A. Almogren, "Increasing the trustworthiness in the industrial IoT networks through a reliable cyberattack detection model," IEEE Transactions on Industrial Informatics, vol. 16, no. 9, pp. 6154–6162, 2020.

[7] F. Reegu, W. Khan, S. Daud, Q. Arshad, and N. Armi, "A reliable public safety framework for industrial internet of things (IIoT)," in Proc. Int. Conf. Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), Serpong, Indonesia, 2020, pp. 189–193.

[8] Swati, S. Roy, J. Singh, et al., "Design and analysis of DDoS mitigating network architecture," International Journal of Information Security, vol. 22, pp. 333–345, 2023, doi: 10.1007/s10207-022-00635-1.

Received: 2026-05-14
Accepted: 2026-07-15
Published Online: 2026-07-20
DOI: 10.70454/JRICST.2026.030303

Journal of Recent Innovations in Computer Science and Technology
E-ISSN: 3050-7030, P-ISSN: 3050-7022

[9] S. Oyucu, O. Polat, M. Türkoğlu, H. Polat, A. Aksöz, and M. T. Ağdaş, "Ensemble learning framework for DDoS detection in SDN-based SCADA systems," Sensors, vol. 24, no. 1, p. 155, 2024, doi: 10.3390/s24010155.

[10] H. Li and G. Xiang, "Research on DDoS attack detection based on SDN architecture," in Proc. 4th Int. Conf. Cryptography, Network Security and Communication Technology (CNSCT), New York, NY, USA, 2025, pp. 75–79, doi: 10.1145/3723890.3723903.

[11] X. Zhang, Y. Song, and C. Ge, "A DDoS attack detection and mitigation system in SDN," in Proc. 14th Int. Conf. Computer Engineering and Networks (CENet 2024), Lecture Notes in Electrical Engineering, vol. 1387, Singapore: Springer, 2025, doi: 10.1007/978-981-96-4245-8_9.

[12] J. A. Pérez-Díaz, I. A. Valdovinos, K.-K. R. Choo, and D. Zhu, "A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning," IEEE Access, vol. 8, pp. 155859–155872, 2020, doi: 10.1109/ACCESS.2020.3019330.

[13] M. Revathi and S. K. Devi, "Hybrid architecture for mitigating DDoS and other intrusions in SDN-IoT using MHDBN-W deep learning model," International Journal of Machine Learning and Cybernetics, vol. 16, pp. 6997–7018, 2025, doi: 10.1007/s13042-024-02147-x.

[14] R. Swami, M. Dave, and V. Ranga, "Mitigation of DDoS attack using moving target defense in SDN," Wireless Personal Communications, vol. 131, pp. 2429–2443, 2023, doi: 10.1007/s11277-023-10544-8.

[15] S. Kautish, R. A, and A. Vidyarthi, "SDMTA: Attack detection and mitigation mechanism for DDoS vulnerabilities in hybrid cloud environment," IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6455–6463, Sep. 2022, doi: 10.1109/TII.2022.3146290.