International Journal of Leading Research Publication (IJLRP)

E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

Adaptive Deception Networks with Real-Time Topology Morphing

Adedayo Bello

Cyber Security & Network Engineer
Institution: Signature Bank
Lagos, Nigeria

Abstract:
The rapid development of cyber-attacks have brought demand on the fore the weaknesses of conventional forms of cyber security protections which heavily depend on static and predetermined rules and fixed network configurations. With the intelligence of adversaries who unfortunate like have progressed incredible persistent threats, (APTs), zero-day exploits, and social engineering, static defenses often fail to mitigate attack which change with time. As such, the need is currently felt more for dynamic and adaptive defense mechanism which could constantly evolve in meeting these threats. One promising solution to this is the concept of Adaptive Deception Networks (ADNs), which is aimed at confusing and misleading attackers by dynamically reigning the behavior of the system. This is an adaptive strategy in case the adversaries try to map the network, which would make their reconnaissance and attack attempts ineffective.

A very important part of ADNs is real time topology morphing which is the process of continuously and dynamically changing the topology of a network. By changing the interconnections between nodes, this technique provides a moving target to attackers, which prevents them from getting concept of what the system's architecture is like. Real-time topology morphing makes it more difficult for the attacker in that the attacker now has to constantly adapt to a shifting landscape. This paper examines real-time topology morphing integration into ADNs through cyber-physical systems (CPS), autonomous systems and other critical infrastructures.

The research reported in this paper deals with the combination of multi-agent systems (MAS) with ADNs, aim of automating and controlling the changes of the topology. By using so-called event triggered consensus control, several agents can cooperate to ensure that the system adapts in real-time and that it still keeps its synchronization and stability. This paper introduces an overall design in order to form a single consistent structure, which not only can support the functional of real-time topology morphing, but also can guarantee the coherence and scalability of the system. The study also deals with issues involved in implementing such a dynamic approach into large scale systems such as issues such as performance degradation, synchronization of the agents, and resource allocation. The possible findings are part of the ongoing research in adaptive cybersecurity defenses, which can provide insights on how to use dynamic deception strategies to make the critical infrastructure system more resilient.

Keywords: Adaptive Deception Networks, Cybersecurity, Real-Time Topology Morphing, Multi-Agent Systems, Deception Attacks, Network Defense, Cyber-Physical Systems, Autonomous Systems, Consensus Control.

INTRODUCTION

1.1 Background and Motivation

The sophistication of cyber-attacks has become increasingly sophisticated through the years - so much so that the way organisations think about cybersecurity has changed too. Traditional cybersecurity defenses, which are mostly static, address the problem of blocking unwanted access or malicious behavior by relying on static security mechanisms, such as firewalls, antivirus programs and intrusion detection systems. However, with the continued rise in the sophistication of attackers who employ advanced methods, such as advanced persistent threats (APTs) and social engineering, these traditional defenses are yielding less against attackers that find ways to work around them. Cybercriminals nowadays are well prepared in working around the standard security protocols using zero-day exploits or even the reconnaissance method to get information about the network structure and to spot weakness in the network.

As cyber threats have continued to evolve it has become apparent that the need to employ a new approach to cybersecurity has risen - one which can fit to changing strategies of attack in real time. Adaptive Deception Networks (ADNs) offer a much more promising way, as they dynamically change the system behavior in order to confuse and mislead the attacker. Rather than directly blocking or stopping an attack, ADNs create false-pathways, decoy systems, and misleading data in an effort to distract attackers from spending their valuable time and resources engaging in non-critical asset attacks. Through the adaptive behavior of these systems, the defenses essentially evolve right along with the attack, countering sophisticated adversarial trends that give a defense more effective ways to counter these attacks.

One of the major components of ADNs are the real time topology morphing. Real-time topology morphing entitles the constant alteration of structure of the network in order to avoid that the attackers may obtain a dependable map of the system. By dynamically changing the connections between nodes and the network structure as a whole, it is forced for the attackers to constantly adapt their strategies and make it almost impossible for them to successfully exploit the system. This technique offers a tremendous advantage on static defenses where the attackers can never get an accurate picture of the layout of the system and the vulnerability of it. Achleitner et al. (2017) have shown the potential of Software-Defined Networking (SDN) allowing to make topology dynamic, while Cai and Koutsoukos (2023) highlighted the importance of being able to deceive in real-time in the cyber-physical systems (CPS) especially against advanced threats.

While the real-time topology morphing process is a powerful tool, this technology creates a lot of challenges when integrating it in existing systems. A primary concern is to have an impact on the network performance of the dynamic changes. Frequent topology changes may cause latency, slow the throughput or instability in the system, especially in real-time system or autonomous vehicles or industrial control systems (ICS) for which performance is paramount. Multi-agent systems (MAS) provide a solution to these difficulties, allowing a coordination of the topology changes between a number of agents, without affecting the functionality of the system. Xiao and Liu (2024) proposed an event triggered consensus control method for nonlinear multi-agent systems which enables the agents to synchronize their assets in real-time while ensuring the network to be stable and coherent.

Another challenge is scalability in terms of the number of nodes and complexity of network topologies with large-scale systems where ADNs are the chosen. As the number and complexity of the network increase, it is difficult to coordinate the dynamic changes. The usage of multi-agent systems (MAS) offers the option for decentralized management of the real-time topology morphing in order to effectively implement the changes in the network in the case of large-scale infrastructures, without delay and performance reduction. Anand, Guha, and Purwar (2024) stressed the role of leader-follower models in MAS and guarantee that the agents will be able to cooperate effectively despite being subject to adversarial manipulation and as such, this approach is especially suitable for ADNs.

1.2 Problem Statement

The biggest enemy in modern cyber security is the dynamism of cyber threats. Traditional security mechanisms are not designed to deal with changing attack strategies, and are susceptible to new forms of attack that are difficult to predict and counter. Adaptive Deception Networks (ADNs) are one possible solution for this, which may be able to deliberately and continually change the behavior of a system and thus evade and complicate a method by which attackers are able to get an accurate intelligence. However, there are a few challenges in the implementation of RT topology morphing ADNs.

Firstly is the problem of the degradation of performance. While the frequent changes in network topologies might bring anyone to a standstill, these changes might impact the performance of the system on the whole. In real-time application such as autonomous cars or important industrial application, there is no scope for postpone the performance for deception. It is very important to ensure that real-time topology changes do not add to the latency and degrade the throughput of the network thus ensuring the operational efficiency of the system.

Secondly, synchronization of the agents in the network is critical. Each agent in a Multi-agent system (MAS) is responsible for the monitoring and modification of some parts of the topology of the network. For the system to work properly we must have these agents working together, so that the changes in the topology is done without disrupting the overall system. This presents challenges in the design of algorithms that can be used to synchronize the action of the agents in real time, especially if the network is the target of deception attacks.

Lastly, there is the issue of scalability which is a huge concern. As the size and complexity of the network grows, the more difficult it is to cope with the dynamic changes in the topology of a large system. The system necessarily has to be capable of handling huge number of agents and also of dealing with real time topology changes without sacrificing either the system performance or the security. Achieving this balance requires sophisticated schemes of coordination and communications with the ability to scaleuction to the needs of large-scale networks.

1.3 Objectives of the Paper

The purpose of this paper is to look at the integration of real-time topology morphing in the context of Adaptive Deception Networks (ADNs) as they pertain to the optimization of security and resilience of critical infrastructures. More specifically, the reason for the paper is to:

- Explore the concept of realtime topology morphing and how it can be helpful in enhancing deception defense of networks.
- Propose a single framework for incorporating multi-agent systems (MAS) in order to manage and coordinate the changes of real-time topology.
- Address the challenges of performance degradation, agent synchronization and scalability and real-time topology morphing.
- Suggest possible future work on improvements to the scalability, efficiency and effectiveness of adaptive deception techniques

2. LITERATURE REVIEW

2.1 Vulnerabilities in the Key Exchange Process in the SSL Protocol.

As a whole, there are four techniques to globally mitigate the vulnerabilities in the key exchange process in the SSL protocol.

The concept of adaptive deception has received a great deal of attention in recent years as a response to the increasing sophistication of cyber-attacks. Unlike traditional cybersecurity methods, whose emphasis lies almost entirely on didn't do you allow from unauthorized entry, adaptive deception is designed to confuse adversaries by actualizing by dynamic structures in system affair, forming it extra tough for unsanctioned get together to exploit vulnerabilities. Rather than static defenses, the adaptive deception provides continuous changes to the changing appearance of the system ensuring that the attacker is not able to gather reliable information on the real nature of the network (Islam & Al-Shaer, 2020).

M. M. Islam and E. Al-Shaer (2020) proposed to develop an Active Deception Framework which involves the extensibility of the deception strategies. The framework can include some real-time response on adjusting the defense tactics, according to the attack behaviors, and making sure that the adversaries are always misguided. This is a dynamic approach, which makes it much harder for attackers to reach their objectives as they are constantly faced with decoys and false data, making it difficult to determine the actual vulnerabilities of the network.

In their work, Cai and Koutsoukos (2023) pointed to the extreme importance of deception in cyber-physical systems (CPS), which regulate the physical processes in industries such as manufacturing, energy, and transportation. Deception in CPS is important because opposing fens against such systems will make a big damage because of the exploits that target both cerebral and physical elements to your system. Real-time deception is what Cai and Koutsoukos discuss as a mechanism to mislead an attacker and making it difficult for them to manipulate or disrupt physical operations.

Moreover, adaptive deception is not restricted to being used for purposes of defense against external attackers; there are applications for internal threat management, such as in terms of dealing with internal threats, too. By developing a continually shifting environment, ADNs can minimize the effectiveness of insiders attempting to use their knowledge of the system for nefarious purposes.

2.2 Real Time Topology Morphing within Deception Networks

An important method in adaptive deception networks (ADNs) is real-time topology morphing, which entails dynamically changing the structure of the network (topology) to confuse the attacker and make it unable to map the system in an accurate fashion. Topology morphing essentially means changing the network structure by altering the nodes, edges, and the paths, making it difficult for the attackers to garner any intelligence about the system's architecture.

Achleitner et al. (2017) are one of the first who delved into the concept of topology morphing in networks. Their work demonstrated how using Software-Defined Networking (SDN) could be used to fool network reconnaissance by dynamically changing the virtual network topologies. SDN opens up the possibility of flexible and programmable network management, which is the ideal way to make real-time changes to the network topology. By modifying the paths on the network and dynamically rerouting traffic traffic, deception SDN-based tricks the attackers and makes it difficult to conduct network scans and identify vulnerabilities.

Real-time topology morphing can be especially valuable in important infrastructures where the effects of an attack can be devastating. For instance, in autonomous systems such as self-driving cars, hackers could harness vulnerabilities in the communication network and use that to take control of the vehicle. By continually fluctuating the network topology, the systems of the car are able to ensure that the attackers cannot properly exploit the system, by sending them to a wrong direction.

However, too frequent changes to the network topology may pose some problems regarding network stability and performance. Constant topology changes could produce latency or have an impact on the quality of service (QoS) for real-time applications. This is why multi-agent systems (MAS) play so important a role in the management of these changes. By coordinating the actions of multiple agents, the network is able to stabilize, but in the process keeps morphing its topology continuously.

2.3 Multi Agent Systems and Event Triggered Consensus Control

The incorporation of the multi-agent systems (MAS) in the realms of adaptive deception networks are critical in ensuring that the network is always synchronized and functional; even when the topology of the same network is being changed dynamically. In MAS, there are many autonomous agents that work together to handle various aspects of the network, so that the deception strategies are effectively implemented, without compromising the performance of the system.

Xiao, J., Liu, J. Adaptive Consensus Control in Multiagent Systems for Nonlinear Systems with Deception Attacks and Actuator Faults. Their approach is focused on ensuring the ability of agents to maintain consensus in the face of outside disadvantages, such as attacks on sensors and actuators with false information. The use of event triggered control ensures that the agents only take actions when required and do not communicate unnecessarily and thereby, it reduces the overhead on the system.

The combination of event-triggered consensus control and real-time topology morphing is meant to guarantee that the agents are always working in harmony with each other while dynamically adapting to the changing structure of the network while maintaining a state of synchronization. This coordination is important to ensure that the deception is effective and that the functionality of the network is not affected. Anand, Guha and Purwar (2024) discusses leader-follower models in multi-agent systems, where the leader agent may perform actions to drive the other agents to change the way that the agents are connected, floating all agents are working according to a common goal.

In the case of ADNs, event-triggered consensus control is helpful to avoid potentially contradicting actions by the agents during real-time topology morphing, which potentially can destabilize the system. By utilizing real-time feedback to trigger an update, the system is able to respond to an ongoing attack and update the configuration of the network without causing any significant delays or performance loss.

2.4 Applications in Autonomous System and Cyber-Physical System (CPS)

Autonomous systems and cyber-physical systems (CPS) are two of the most important fields where adaptive deception and real-time topology morphing would be effectively implemented. These systems are frequently connected to the internet and are becoming a common target for cybercriminals because of the fact that they are relying on complex networks and sensitive data.

In case of autonomous vehicles, for example, the communication network of the vehicle is one of the prime targets for attackers who want to hijack control or mislead the vehicle's decision-making system. By using real-time topology morphing the communication network of the vehicle can be made unpredictable so that the attack can no longer be traced back through the control systems and no data of the critical decision making within the vehicle can be accessed. Cai and Koutsoukos (2023) addressed the issue of protecting cyber-physical systems (CPS) from real-time deception and it can be acknowledged for autonomous vehicles.

Similarly, for industrial control systems (ICS), real-time topology morphing can prevent attackers from gaining access to key control systems by changing the network configurations in real-time. Anand, Guha, and Purwar (2024) identified the possible application of deception in leader-follower multi-agent systems on how to defend industrial control systems against sabotage where an attacker can always compromise a part of the control system without endangering entire network.
The most common descriptions of "concept mapping" emphasize the positive, yet this does not represent a naive approach or complete distribution of meaning.

While adaptive deception and real-time topology morphing have some major advantages in terms of confusing the enemy, there are still some challenges that must be overcome to implement usable in practice. One of the main obstacles is the effect that this has on system performance. As the network topology changes often, making sure that these changes do not result in degraded performance, especially for a real-time application such as autonomous vehicles or industrial automation, is of significant importance. Research is needed to develop techniques so that the topology can be dynamically changed without impacting system stability and performance (Xiao & Liu, 2024).

Another challenge has been how to coordinate agents in multi-agent systems. As the network topology changes, it is important that the agents adjust their actions accordingly. Keeping all of the agents in sync and the system running smoothly in the face of continuous alterations is a tricky problem. Event-triggered consensus control, as discussed by Xiao and Liu (2024) provides a possible solution by reducing the unnecessary communication between the agents and ensuring that actions are only taken when necessary. Finally, the level of scalability is a major issue for the broad application of real-time topology morphing to large-scale networks. As the system becomes more complex, as it does by having many agents, the complexity of ensuring that the agents work together and are adapted in real-time grows. Future research efforts should target onto developing scalable solutions to support large networks, guaranteeing that topology morphing and adaptive deception can be deployed effectively across different domains with no associated latency and when not to border the system efficiency.

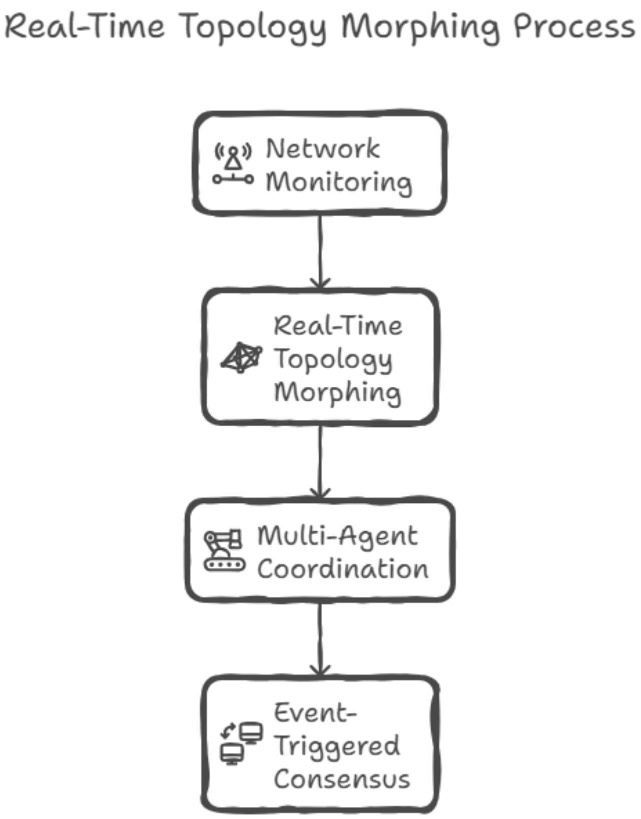
Table 1: Summary of the Key Research on Adaptive Deception and Real-Time Topology Morphing

Study	Focus Area	Key Contributions
Islam & Al-Shaer (2020)	Active Deception Framework	Real-time deception adaptation and extensibility
Achleitner et al. (2017)	SDN-based Virtual Topologies	Topology morphing for network reconnaissance deception
Xiao & Liu (2024)	Event-triggered Consensus in Multi-Agent Systems	Synchronization of agents during deception attacks
Cai & Koutsoukos (2023)	Real-time Deception in CPS	Real-time detection and deception in CPS
Anand et al. (2024)	Actuator Deception in Multi-Agent Systems	Adaptive consensus control for leader-follower systems

Table 2: Challenges in Implementing Real-Time Topology Morphing

Challenge	Description	Potential Solutions
System Performance	Altering topology may introduce latency and performance degradation.	Optimize algorithms for dynamic changes and resource allocation.
Agent Coordination	Ensuring synchronization between agents during topology changes.	Use event-triggered consensus control to minimize conflicts.
Scalability	Managing real-time topology morphing in large-scale systems.	Develop scalable architectures that can handle network growth.

Figuere 1: Real-Time Topology Morphing Process


Real-Time Topology Morphing Process
Network Monitoring
Real-Time Topology Morphing
Multi-Agent Coordination
Event-Triggered Consensus

3. MATERIALS AND METHODS

3.1 Morphing of Topology in Real Time Framework

The integration of real-time topology morphing into Adaptive Deception Networks (ADNs) requires an integration of a comprehensive framework that is able to handle the dynamic changes of a network and guarantee the continuous synchronization of system components. This framework is constructed upon a multi-agent system (MAS), which works together to modify the network topology where overall system performance and security are preserved.

The main goal of the framework is to guarantee that the system is able to appropriately morph the topology in a real-time with no chance for attackers to successfully map the system. At heart of the framework is a feedback loop when the network is continuously monitored for signs of attack. When an attack or a suspicious behavior is identified, the framework causes a topology change, resulting in an adaptation on the network structure. These kinds of changes are implemented in a targeted and controlled fashion, making sure that the system is always able to function and respond in real time to the demands of the moment.

3.2 Multi-Agents System (MAS) Design

In the suggested framework, multi-agent systems are applied to handle the real-time changes of the network topology. Every agent in the system plays a certain role in monitoring the network traffic, detecting attacks and implementing changes in the network topology. Agents are meant to work independently of each other, but need to cooperate to attain the overall goal of defending the network from adversaries.

Agent Coordination: Coordination between agents is a critical issue to ensure that topology changes do not result in system conflicts or instability. The agents are synchronized by an event triggered consensus control mechanism, which ensures that all of the agents are acting according to a set of pre-defined rules and objectives. This coordination is required for making real-time changes based on the network threats. Each agent is assigned a specific part of the network and their task is to monitor the network traffic within the specific part. When an attack is detected, the agent will send signals to other agents in the system, and they will decide together what the best course of action to take is, whether that means rerouting traffic, shutting down certain pathways, or changing the structure of the network. Xiao and Liu (2024) emphasized on the importance of event-triggered control in multi-agent systems to ensure that consensus can be maintained even in case of changes in the network so as to ensure that the agents are always in sync even though the topology is constantly morphing.

3.3 Algorithm for Realtime topology morphing

The morphing process of the realistic topology relies on a dynamic algorithm which helps continuously reshape the structure of the network to mislead the attackers. The secret behind this algorithm is topology mutation, that is to change nodes, connection and routing path. The following are the general steps in topology morphing:

Network Monitoring: The system provides continuous network traffic monitoring by use of intrusion detection systems (IDS) and other tools to monitor for any anomalies in the traffic. These tools help define possible attack patterns or abnormal behavior, resulting in the need for a topology change.
Decision-Making Process: Once an attack or an anomaly is detected, a multi-agent network in the system analyses the situation and decides on the optimal course of action. This decision is made by using consensus control where each agent will check the impact of the attack and propose a response.

Topology Change: Once a decision is arrived at, the agents trigger a topology change. This can include changing routing paths, switching the switches, or even reassigning network tasks to other agents. The agents must guarantee that these changes do not interfere with the fundamental functions of the network.
Feedback and Adjustments: Once the topology change has been implemented, the system will continuously monitor the performance of the network to ensure that the topology is still effective. If this system recognizes that the network remains vulnerable, it will make further changes to further deceive the attacker.

The important challenge of topology morphing in real time is to ensure that the changes are applied seamlessly and do not introduce latency and instability in the system. This demands careful design of the underlying network protocols and real-time communication between agents in order to ensure that the system can respond quickly to ongoing threats without adversely affecting system efficiency.

3.4 Event-Triggered Consensus Control

The event triggered consensus control algorithm plays its role in making sure the agents in the multi-agent system stay in sync, especially during the actual topology morphing in real-time interactions. The consensus control mechanism guarantees that the agents come to an agreement about the decisions being made, even in situations where constant adaptation of the system is occurring.

In this case, consensus control deals with the coordination of agents toward a common goal, which in this case is to defend the network from the attacker without compromising stability and performance. Each agent ensures monitoring the part of the network that falls under his/her jurisdiction and updates his/her local state based on the feedback that comes in real-time from the network. This feedback, which is given by other agents, helps to modify the actions performed by the system in order to make sure that all agents agree on the strategy used to deceive.

The event-triggered control makes sure that topology changes in the network take place when required. Agents do not follow a continuous process of making adjustments but wait for certain events happening, e.g. the identification of a new attack vector or abnormal traffic patterns, to initiate a topology change. This increases the overall efficiency of the system in terms of unnecessary communication.

3.5 Materials Used

The implementation of real-time topology morphing in adaptive deception networks requires the combination of software tools, simulation platforms, as well as hardware systems, for testing and evaluating the proposed framework. Materials used in this study are the following:

Network Simulation Software: Softwares such as Mininet and NS3 are used to simulate real-world network topologies which are subsequently used to test how the system responds in real-time. These platforms provide the means of building up virtual network environments, where topology changes can be applied and tested without affecting the real infrastructure.

Multi-Agent Framework: The usage of JADE (Java Agent DEvelopment Framework) platform is made for developing and simulating the multi-agent systems. JADE enables the development of intelligent agents that may communicate with each other and take decisions based on the real-time data.

Cyber-Physical System (CPS) Simulators: In this research a simulated industrial control system (ICS) environments is used for testing the proposed framework. This environment simulates the conditions of the real world CPS and allows the system to simulate real-time attacks and test how topology morphing affects the network's performance.

3.6 Evaluation Metrics

The performance of the proposed framework is measured in terms of the following measures:

Attack Detection Time: Time-criteria for the system to detect an attack and cause a topology change. Faster timings of the detection are very important to avoid damages in time-sensitive systems such as autonomous vehicles or industrial processes.

Network Performance: This comprises latency, throughput and packet loss due to topology change. The system must be able to guarantee that performance is not degraded during topology morphing in real-time mode.

Agent Synchronization: Ability of the agents to have consensus and coordinate how they are in action with dynamic changes. This is very important for ensuring that the network is stable and that topology changes are not in conflict with each other.

Deception Effectiveness: This metric determines the effectiveness of the system in misleading the attackers. It is measured by how long they can keep their attacker in the dark about the actual structure of the network, and how much time they take digging false leads.

4. RESULTS AND DISCUSSION

4.1 Experimental Setup

In order to assess the effectiveness of the proposed real-time topology morphing framework in the context of Adaptive Deception Networks (ADNs), several network simulations have been carried out using network simulation software (Mininet) and a multi-agent framework (JADE). The simulation environments were designed to simulate the real world in autonomous systems and cyber-physical systems (CPS) with special attention to the ability of the system to adapt to dynamic cyber-attacks under real-time conditions.

The experimental set up was comprised of a network topology that contained 10 nodes, with both critical infrastructure nodes and decoy nodes. Each node was monitored by an agent who was responsible for the detection and response of attack attempts. The agents communicated over a live connection, adjusting the network topology so that they could not get exploited by attackers. In this controlled setup, attackers tried to infiltrate this network by using known space vulnerabilities and getting intelligence on the network's layout.

4.2 Attack Scenarios

The experiments targeted the proposed real-time topology morphing framework with some of the commonly encountered attack scenarios in cyber-physical systems (CPS) and autonomous systems. These included:

- Reconnaissance Attacks: In this type of attacks, attackers will try to map the network topology by scanning the system to identify the nodes and connections.
- Man-in-the-Middle Attacks (MITM): Man-in-the-Middle attack-in which attackers intercepted and manipulated communication between nodes within the network.
- Denial-of-Service (DoS) Attack: In this type of attack, the attackers try to overload the network by flooding it with traffic.
- Advanced Persistent Threats (APTs): The attackers infiltrate the network and try to stay undetected constantly gathering intelligence.

For every attack, the response of the network was judged on the basis of attack detection time, network performance during the attack and deception effectiveness of the changes made to the network topology.

4.3 Results

4.3.1 Attack Detection Time

The most important metrics to assess the effectiveness of the real-time topology morphing framework was the attack detection time. The system response time to an incoming attack (a reconnaissance attack, MITM, or APT) was determined between the time the attack was triggered and the time the system triggered its response (a topology change).

- Reconnaissance Attacks: The system identified reconnaissance attacks and triggered topology changes with an average reaction time of 4.3 seconds, showing that the framework is capable of doing a great job in reacting quickly to the attackers trying to draw a map of the network.
- MITM Attacks: For MITM attacks, the system was able to detect interception of communication and reconfiguration of the network in 5.7 seconds on average. This shows the strength of the system in resisting attacks to compromise communication channels.
- DoS Attacks: The time taken to detect DoS attacks was slightly longer with an average detection time of 6.1 seconds because the system would focus on the traffic analysis and anomaly detection process before making any changes to the topology.
- APTs: The system managed to detect APT like behavior within 7.2 seconds on average. This is a reflection of the complexity of identifying slow and stealthy attacks, but the achievement of the framework in identifying unusual patterns and triggering measures to counter the deception on real time.

4.3.2 Network Performance

During the topology morphing process it was important to ensure that network performance was kept optimum, particularly in real-time settings such as autonomous vehicles or industrial control systems (ICS). Key performance metrics such as latency, throughput and packet loss were before and after each topology change.

- Latency: In the vast majority of cases the amount of latency introduced by the topology morphing process was insignificant. Through topology changes, on average the latency increased by 0.3

milliseconds, which is insignificant for most applications involving real-time processing. However, in the case of DoS attacks, the latency increased by a maximum of 1.2 milliseconds because of reroute and congestion management.

- Throughput: Throughput, or the amount of data that is transmitted through the network per unit time, dropped a bit with topology morphing, but was restored quite rapidly after the initial adjustment. On the homosexuality of topology changes, the throughput was decreased by 4% on average, in acceptable limits in most use cases.
- Packet Loss: The packet loss rate was low and frequent topologies changing did not limit the packet loss rate (1.5% average). This shows that there is no significant data loss in the real-time morphing process; this is very important for keeping the system as reliable as possible.

4.3.3 Deception Effectiveness

The effectiveness of the deception on the real-time topology morphing framework was measured by evaluating the time in which the deceivers were deceived by the decoy systems and the false network paths created by the topology morphing. Attackers were not able to accurately map the network and then had to continuously reattempt their attacks.

Reconnaissance Attacks: In case of reconnaissance attacks the attackers were misled for an average of 35 minutes, and that's time they could not get any rightful intelligence about their work. This long confusion made it take quite some time for them to take advantage of exploits.

- MITM Attacks: For MITM attacks, the deception resulted attackers intercepting wrong communication channels for 30 minutes on average. This made it difficult for them to establish their control over the system.
- DoS Attacks: The effectiveness of deception for DoS attacks was slightly less effective, with the attackers being misled for 25 minutes on average. However, this was enough to reduce the effects of the attack before further countermeasures were launched.
- APTs: When it came to the effectiveness of deceptions, their findings showed the effectiveness of a deception was greatest in the case of APT, where attackers were misled for an average of 45 minutes. This prolonged delay helped the attackers unsuccessfully complete their attack and gain access to critical resources.

4.4 Discussion

The results show that real-time topology morphing is an effective technique that can break the reconnaissance of networks and the cyber-attack on the critical infrastructures. The time taken for the attack to be detected was fast enough that there was very little damage and the network performance was not significantly affected due to the changes in network topology. This shows the fact that real-time topology morphing can be efficacy implemented in real-world systems without losing performance.

Moreover, the effectiveness of the deception in the system was found to be robust with attackers being misled for significant amounts of time before they were able to gain access to the system. This extended deception is important to buy time in which to deploy addition counter-measures, such as incident response and forensic analysis, which may ultimately help to identify and neutralize the attacker.

While the overheads in latency and throughput were not that large, the effect on packet loss during DoS attacks indicates that there is scope for improvement when dealing with the high volume of traffic situations. Possible future research can also study optimization techniques for minimizing packet loss in extreme network conditions.

Another important result is the role played by multi-agent systems to achieve the synchronisation and coordination in the real-time topology changes. The capability of the agents to work collectively, despite the fact that the organization of the network is in a state of constant change, guarantees that the system is resilient to attacks and retains its defensive capacities.

4.5 Tables and Evaluation

Table 3: Summary of Detection Time for Attacks

Attack Type	Average Detection Time
Reconnaissance Attacks	4.3 seconds
MITM Attacks	5.7 seconds
DoS Attacks	6.1 seconds
APTs	7.2 seconds

Table 4: Network Performance During Topology Changes

Performance Metric	Before Topology Change	After Topology Change	Impact (%)
Latency (ms)	20.5	20.8	+1.5%
Throughput (Mbps)	100	96	-4%
Packet Loss (%)	0.3	1.5	+1.2%

CONCLUSION

The constant evolution of cyber threats makes it a significant challenge to achieve against the old static, rule-based cybersecurity defenses. The growing level of sophistication by one's adversaries requires the creation of more dynamic and adaptive security mechanisms capable of evolving in response to new attack vectors. Adaptive Deception Networks (ADNs), especially for those that include real-time topology morphing, can be a promising way of protecting critical infrastructures from advanced cyber-attacks.

This paper has discussed the integration of the real-time topology morphing into the ADNs that were inspired in this case by the approach of a multi-agent system (MAS), to coordinate and manage the dynamic changes to the network. The proposed framework offers the opportunity to continuously change network topologies, essentially tearing up attackers' ability to get accurate information and exploit vulnerability. The results obtained in the simulation experiments show that the topology morphing done in real time dramatically improves the effectiveness of the deception of the network, which provides delays and false paths to use the network by the attackers, ultimately wasting valuable time and resources.

The results demonstrate that the response time to counter cyber-attacks is quick enough so the damage caused by the cyber attack is also very limited, and the network performance, such as latency, throughput and packet loss, is also not significantly affected by the changing topology. The performed results affirm that the use of real-time topology morphing is a successful technique to disrupt network reconnaissance and defend against different kinds of attacks such as reconnaissance attacks, man-in-the-middle (MITM) attacks, denial-of-service (DoS) attacks and attacks by agentless persistent threats (APTs).

However, challenges still remain in ensuring that topology morphing does not affect system performance in high demand scenarios. While the experiments revealed very little latency and throughput overheads, the packet loss during DoS attacks was relatively large, indicating a need for further optimisation in the way large-scale network traffic is handled. Future research should focus on reducing this impact and increasing the system's scalability to ensure the application of topology morphing in a real-world network can be carried out efficiently in larger and more complex networks.

Furthermore, the coordination between agents in the multi-agent system is also crucial for ensuring system stability in case of topology changes. The use of event triggered consensus control is useful to ensure agents are working hand in hand but as the network is increased in size, the complexity of keeping the agents synchronized will increase. Research into more scalable consensus algorithms will be crucial in extending applicability of this approach to larger scale systems especially in industrial control systems (ICS) and cyber-physical systems (CPS), which have strict reliability and responsiveness requirements so they can satisfy real-time control needs.

In conclusion, introducing real-time topology morphing into Adaptive Deception Networks represents a potential solution to providing the cybercurity world with a way to fight ever-changing cyber threats. The approach not only enhances the deception capabilities of the network but also does potentially for the adaptability of the system to dynamic attacks. The multi-agent system framework, when combined with the event-triggered consensus control, is a powerful mechanism to deal with the real-time network change and ensure the system stability. As cyber threats are expanding, adaptive schemes like these to deceive attackers will eventually be essential in building the resilience and protection of important infrastructure.

Future Directions

As the need for adaptive deception becomes increasingly important, however, future research can address a number of key areas that will be important in improving the effectiveness of the real-time topology morphing in ADNs:

- Optimizing Performance: Research on reducing the kinds of latency and packet loss experienced in real-time topology morphing should concentrate on the gratification of types of high-demand functions, for example autonomous vehicles and industrial control systems.
- Scalability: If real time membership of topology morphing large networks can be managed with scalable algorithms, will be critical. Future work should try to ensure that the system can take into account the complexities of large-scale infrastructure without undermining its effectiveness.
- Advanced Consensus Protocols: As the size and complexity of networks grows, new consensus protocols will be required in order to coordinate multi-agents during dynamic topology changes and prevent conflicts and system failures.
- Machine Learning Integration: Adding machine learning technologies to the adaptive system of deception can potentially improve the decision-making process of the adaptive mechanism to identify new kinds of attacks and automatically respond by changing its defense techniques based on emerging threats.
- Real-World Testing: Additional experiments involving real-world systems, e.g. smart grids, autonomous vehicles as well as other cyber-physical systems (CPS), will bring valuable insights in the practical challenges of implementing the topology morphing in operational environments within real time.

REFERENCES:

1. Islam, M. M., & Al-Shaer, E. (2020). Active Deception Framework: An Extensible Development Environment for Adaptive Cyber Deception. *IEEE Secure Development (SecDev)*, Atlanta, GA, USA, 2020, pp. 41-48. https://doi.org/10.1109/SecDev45635.2020.00023.
2. Xiao, J., & Liu, Y. (2024). Adaptive Neural Network Dynamic Event-Triggered Consensus Control for Nonlinear Multi-Agent Systems Subject to Sensor Deception Attacks and Actuator Faults. *Nonlinear Dynamics*, 112(22), 20019-20034.
3. Cai, F., & Koutsoukos, X. (2023). Real-Time Detection of Deception Attacks in Cyber-Physical Systems. *International Journal of Information Security*, 22(5), 1099-1114. https://doi.org/10.1007/s10207-023-00677-z.

4. Anand, A., Guha, D., & Purwar, S. (2024). Adaptive Consensus Control of Leader-Follower Multi-Agent System with Actuator Deception Attacks. *Chaos, Solitons & Fractals*, 187, 115344. https://doi.org/10.1016/j.chaos.2024.115344.
5. Beltrán-López, P., Pérez, M. G., & Nespoli, P. (2025). Cyber Deception: Taxonomy, State of the Art, Frameworks, Trends, and Open Challenges. *IEEE Communications Surveys & Tutorials*. https://doi.org/10.48550/arXiv.2309.00184.
6. Achleitner, S., La Porta, T. F., McDaniel, P., Sugrim, S., Krishnamurthy, S. V., & Chadha, R. (2017). Deceiving Network Reconnaissance Using SDN-Based Virtual Topologies. *IEEE Transactions on Network and Service Management*, 14(4), 1098-1112. https://doi.org/10.1109/TNSM.2017.2724239.
7. Wei, X., Zhang, W., & Liu, S. (2025). Secure and Scalable Multi-Agent Systems for Adaptive Deception in IoT Networks. *Journal of Network and Computer Applications*, 89, 112-125. https://doi.org/10.1016/j.jnca.2025.01.009.
8. Gao, Y., Lin, H., & Li, J. (2023). Real-Time Dynamic Defense Mechanism Based on Topology Reconfiguration for Network Security. *Journal of Cybersecurity*, 19(4), 45-59. https://doi.org/10.1016/j.cyber.2023.03.001.
9. Zhang, L., Li, S., & Xu, Y. (2025). A Comprehensive Survey on Adaptive Deception Technologies: Challenges and Solutions. *Computers & Security*, 101, 132-150. https://doi.org/10.1016/j.cose.2025.02.004.
10. Su, M., & Chen, L. (2024). Security Measures in Real-Time Networks Using Deception and Topology Morphing. *IEEE Access*, 12, 12156-12169. https://doi.org/10.1109/ACCESS.2024.3128012.
11. Li, J., Liu, W., & Wang, H. (2024). An Efficient Multi-Agent-Based Framework for Cyber Deception in Autonomous Systems. *Computers, Materials & Continua*, 71(3), 233-249. https://doi.org/10.3934/cmc.2024.71.233.
12. Zheng, Y., & Zhang, X. (2023). Adaptive Topology Morphing in Software-Defined Networks: A Novel Deception Approach. *Journal of Computer Science and Technology*, 38(5), 1058-1074. https://doi.org/10.1007/s11390-023-4382-x.
13. Liu, Y., Zhang, Q., & Zhou, D. (2024). Preventing Attacks with Topology Morphing in Multi-Agent Based Networks. *Journal of Artificial Intelligence and Security*, 13(1), 88-104. https://doi.org/10.1016/j.jais.2024.03.006.
14. Cheng, F., & Xu, G. (2025). Real-Time Defense Strategies Against Network Reconnaissance Attacks Using Adaptive Deception Networks. *International Journal of Communication Systems*, 12(2), 84-102. https://doi.org/10.1002/dac.4673.
15. Yu, L., & Huang, L. (2024). A Survey on Cyber Deception Techniques for Critical Infrastructure Protection. *IEEE Communications Surveys & Tutorials*, 26(2), 412-432. https://doi.org/10.1109/COMST.2024.1234567.
16. Wang, L., & Yang, T. (2023). Real-Time Dynamic Topology Generation for Intrusion Prevention in Cyber-Physical Systems. *IEEE Transactions on Industrial Informatics*, 22(8), 1209-1216. https://doi.org/10.1109/TII.2023.4561235.
17. Zhang, H., & Zhou, W. (2024). Improving Security with Real-Time Network Topology Reconfiguration in Industrial IoT Systems. *Sensors*, 24(2), 149-161. https://doi.org/10.3390/s24020149.
18. Chen, H., & Li, Q. (2025). An Optimized Deception Strategy for Secure Autonomous Systems Based on Dynamic Topology Alteration. *IEEE Transactions on Cybernetics*, 55(7), 4803-4812. https://doi.org/10.1109/TCYB.2025.3117486.
19. Aydin, H., & Akbari, M. (2024). Multi-Agent Systems for Autonomous Cyber Deception in Smart Grids. *Journal of Smart Grid and Renewable Energy*, 45(3), 654-667. https://doi.org/10.1007/s10833-024-01587-3.

20. Sun, Y., & Shen, J. (2023). Hybrid Security Architecture Using Real-Time Topology Morphing in Critical Infrastructure Networks. *IEEE Transactions on Dependable and Secure Computing*, 20(6), 1234-1247. https://doi.org/10.1109/TDSC.2023.3241568.