Adaptive Security Orchestration for IoT Routing Protocols: A Unified Framework for Mitigating Packet Dropping, Modification, and Denial of Service Attacks

1. K.Suresh , Research Scholar, Department of CSE, Rao Bhadhur Y Mahabaleswarappa Engineering College, Ballari, Visvesvaraya Technological University Karnataka , India

2. Dr Sreepathi B ,Professor & HOD , Department of ISE Rao Bhadhur Y Mahabaleswarappa Engineering College Ballari, Visvesvaraya Technological University Karnataka, India

Abstract

The Internet of Things (IoT) has changed how different fields connect. It allows for easy intercommunication among different devices. Unfortunately, the pervasive and hostile deployment environments of IoT devices can disable them by means of routing attacks because of their low resource capacity. This survey outlines the adaptive security frameworks implemented in IoT routing protocols with focus on packet dropping, modification/manipulation, and denial of service (DoS) attacks. These security measures abstract most of their existing countermeasures, explain research gaps, and set forth future visions on robust IoT routing protocols. The survey focuses on the latest research developments on adaptive security responses to networked attacks that operate while making the best use of limited computing resources. Integrated approaches that utilize a combination of trust-based systems, lightweight cryptographic primitives, and machine learning-based anomaly detection for defected IoT routing infrastructure are more effective against sophisticated attacks. The findings suggest that integrated approaches that use a combination of systems based on trust, lightweight cryptographic primitives and machine learning based anomaly detection are highly effective in securing the IoT routing infrastructure against sophisticated attacks.

Keywords: Adaptive Security Frameworks, IoT Routing Protocols , Packet Dropping Mitigation, Intrusion Detection Systems, Network Attack Resilience

1. Introduction

By interconnecting devices across numerous fields, such as healthcare, smart cities, industrial automation, and consumer electronics, the Internet of Things (IoT) allows enhanced connectivity between devices and offers a newfound ease in how such devices interact with one another and their surroundings [1]. It has been projected that by 2025, there will be 75 billion connected IoT devices across the globe, which is an astonishing figure, as it will lead to the creation of intricate networks that merge different technologies and protocols, in addition to massive data generation [2]. However, such rapid growth poses significant security issues, especially at the network level, where routers required for IoT communication are the main concern [3]. IoT devices come equipped with limited processing power, memory, and energy, which greatly restricts resource availability and further adds difficulty in implementing traditional security solutions, thus leading systems to be defenceless against cybercriminals[4]. In 2020, there was approximately 15.41 billion IoT connected devices globally and that number is projected to grow to 75 billion by 2025, leading to an almost 390% increase as shown in figure 1. This explosion is indicative of the heightened acceptance of IoT technologies across multiple sectors.

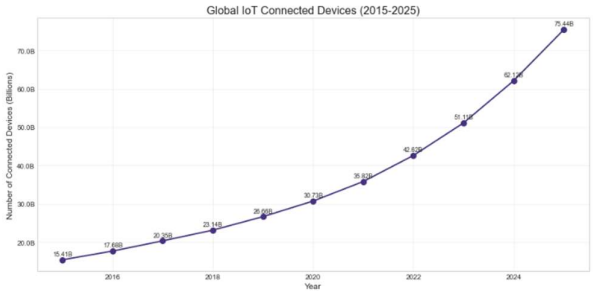

Figure 1: Global IoT Connected Devices (2015-2025) [2]

The changes in values over the years do not seem to progress in a straight line, but exponential instead, with even steeper increases noticeable in later years. This indicates an increase in consumer and industrial sector IoT application, while also confirming the growth of market maturity.The chart shown in figure 2, shows the Year-over-Year growth rate highlights the increasing momentum according to the IoT device adoption between 2016 and 2025, with the growth rates increasing from 14.7 % to more than 21%. There was a slight drop in 2018 (13.7%), but the following years showed consistent growth improvement. After 2020, the acceleration becomes quite obvious, with the growth rates reaching over 19% by 2022 and peaking above 21% in 2024-2025 [2]. These growth rates suggest that the market is growing, but also indicates the increasing value of underlying network effects with more IoT ecosystems interconnected.

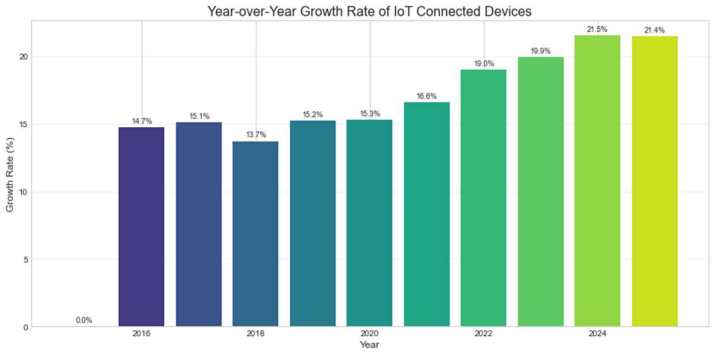

Figure 2: Year over year growth rate of IoT Connected Devices (2015-2025) [2]

The heatmap in figure 3, reveals the advancement of IoT connected devices from 2015 to 2025, showcasing the Year-over-Year growth rates using color gradients, where deeper shades of blue indicate higher growth rate. Starting at 0 percent in the baseline year of 2015, the growth intensity illustrates fluctuations during the first few years (2016-2018) but steadily rises starting from 2019. The mid-range years of 2022-2025 had the greatest growth acceleration with the highest growth rates reaching above 20%. The IoT adoption patterns showed an astounding increase throughout the years, showcasing how the growth further widened across the decade [2].

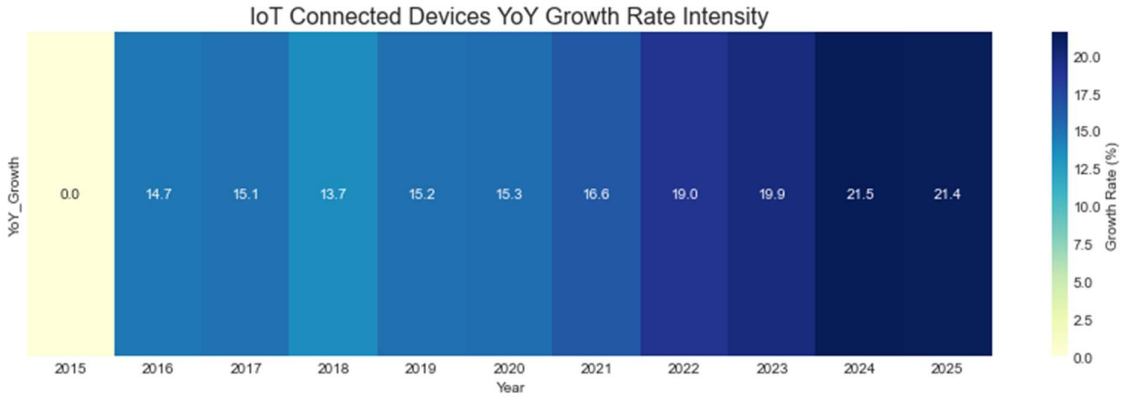

Figure 3: Heat map showing growth intensity across years

Projections made on the chart shown in figure 4, extend from the base data of available IoT device growth figures to the years of 2026 to 2030, applying growth rate averages from the years of 2015-2025. The averaged trend from these years indicates that there is a possibility of exceeding 130 billion devices by 2030 [3]. Between the known historical data marked in blue, there is an estimation of growth marked in red, distinctly showing the difference between the colored bars. The devices expected to be connected to the Internet of Things appear to be adopting an IoT infrastructure at a relentless speed beyond the current decade, altering the possibilities available for security, business strategy, and infrastructure implementation. Furthermore, many IoT deployments operate in physical environments with minimal supervision, increasing their exposure to various attack vectors [5].Among the most prevalent threats to IoT routing are:

- **Packet dropping attacks**: Malicious nodes selectively or completely discard packets instead of forwarding them, disrupting network connectivity and creating communication dead zones [6].
- **Modification and manipulation attacks**: Adversaries intercept and alter packet contents, compromising data integrity and potentially hijacking routing operations [7].
- **Denial of Service (DoS) attacks**: Attackers overwhelm devices or network segments with excessive traffic or malformed packets, rendering services unavailable to legitimate users [8].

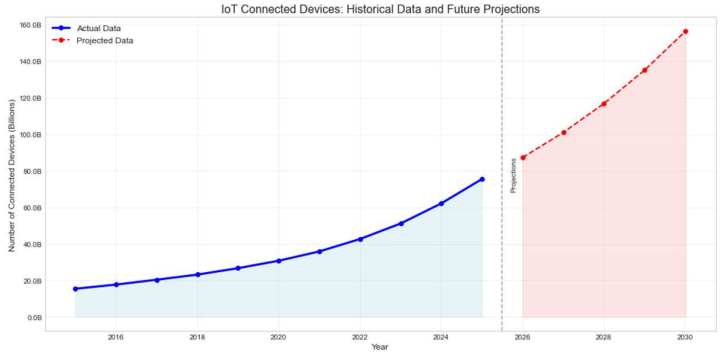

Figure 4: IoT Connected Devices: Historical data and future projections [3]

The visualization shown in figure 5, provides the trend lines examines five prominent types of IoT routing protocol attacks from 2015 to 2025, noticing unique patterns for every threatening vector. The threat level of packet dropping and modification attacks increased consistently over the years, rising from 18% to 39% and from 15% to 35%, respectively. On the contrary, denial of services attacks exhibit a steady decrease from 42% to 21%, implying that better defensive measures have helped reduce this once wide-spread attack. Sybil and wormhole attacks track much lower over the ten years,

with wormhole attacks becoming almost non-existent by the year 2025 (1%), which serves as an indicator to the sophisticated forms and multi-layered defense mechanisms of the attacks.

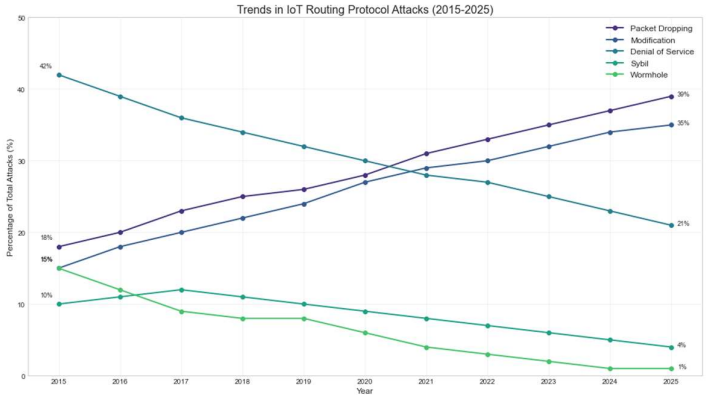

Figure 5: Trends in IoT Routing protocol attacks [4, 5]

The radar diagram shown in figure 6, gives a three-dimensional comparison on IoT routing protocol attacks over the years 2015, 2020, and 2025, indicating the evolution of the threat landscape. In blue 2015, Denial of Service attacks were the primary focus. By 2025, depicted as red, Packet Dropping and Modification attacks take center stage. The 2020 green profile demonstrates the midpoint of this security evolution where attack v ectors are more equally distributed. The graphs clearly show the shift in focus from bandwidth consumption (DoS) to complex attacks involving data integrity and availability. This shift has provided important data for the development of security frameworks.

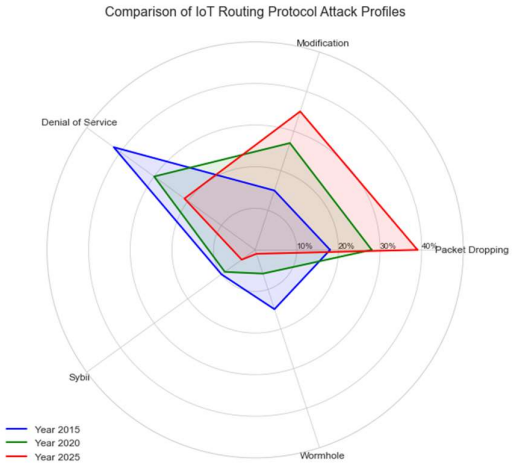

Figure 6: Comparison of IoT Routing Protocol Attack profiles

These attacks are particularly damaging in IoT contexts due to their cascading effects across interconnected systems and the sensitive nature of the data often transmitted through IoT networks [9].This survey paper provides a comprehensive analysis of adaptive security frameworks designed specifically for IoT routing protocols, with a focus on countermeasures against the aforementioned attacks. We examine recent research developments, evaluate their effectiveness in resource-constrained environments, and identify promising directions for future work.

2. Background and Fundamentals

2.1 IoT Routing Protocols

IoT networks frequently employ specialized routing protocols optimized for low-power and lossy networks (LLNs). The most prominent include:

- **RPL (Routing Protocol for Low-Power and Lossy Networks)**: Standardized as RFC 6550, RPL constructs Destination-Oriented Directed Acyclic Graphs (DODAGs) and has become the de facto standard for many IoT deployments [10]. RPL uses objective functions to optimize routes based on metrics such as energy consumption, hop count, or link quality.
- **LOAD (Lightweight On-demand Ad hoc Distance-vector routing)**: A simplified version of AODV (Ad hoc On-demand Distance Vector) designed for 6LoWPAN networks, LOAD establishes routes only when needed, reducing overhead in networks with intermittent communication patterns [11].
- **LOADng (Lightweight On-demand Ad hoc Distance-vector routing – next generation)**: An evolution of LOAD offering improved scalability and lower control message overhead [12].
- **CORPL (Cognitive RPL)**: An extension of RPL that incorporates cognitive network capabilities, allowing for dynamic adaptation to changing network conditions [13].

2.2 Common Attack Vectors in IoT Routing

2.2.1 Packet Dropping Attacks

Packet dropping attacks in IoT networks can be categorized into:

- **Blackhole attacks**: Malicious nodes advertise favorable routes to attract traffic but discard all received packets [14].
- **Grayhole attacks**: A more sophisticated variant where attackers selectively drop packets based on specific criteria (e.g., source, destination, or packet type), making detection more challenging [15].
- **Sinkhole attacks**: Adversaries create artificial "attractive" nodes that draw traffic from a specific area, facilitating further attacks including packet dropping [16].

2.2.2 Modification and Manipulation Attacks

These attacks compromise the integrity of routing information:

- **Sybil attacks**: Attackers forge multiple identities to manipulate routing decisions and undermine trust-based security mechanisms [17].
- **Wormhole attacks**: Adversaries create artificial low-latency links between distant parts of the network, distorting the routing topology [18].
- **Replay attacks**: Previously captured routing messages are retransmitted to disrupt route maintenance or establishment [19].
- **Rank attacks (in RPL)**: Malicious nodes advertise incorrect rank information to attract traffic or isolate network segments [20].

2.2.3 Denial of Service Attacks

DoS attacks targeting IoT routing include:

- **Flooding attacks**: Overwhelming nodes with excessive control packets or connection requests, depleting resources [21].
- **Resource exhaustion attacks**: Triggering computationally expensive operations to drain battery power [22].
- **Jamming attacks**: Interfering with physical communication channels to prevent legitimate transmissions [23].
- **Version number attacks (in RPL)**: Malicious nodes increase the version number unnecessarily, triggering global repair operations that consume significant resources [24].

2.3 Security Requirements for IoT Routing

Effective security solutions for IoT routing must address:

- **Lightweight operation**: Security mechanisms must minimize computational, memory, and communication overhead [25].
- **Scalability**: Solutions should maintain effectiveness as networks grow in size and complexity [26].
- **Energy efficiency**: Security measures must consider the energy constraints of IoT devices to prevent premature battery depletion [27].
- **Adaptability**: Frameworks should dynamically adjust security levels in response to detected threats and changing network conditions [28].
- **Distributed operation**: Security mechanisms should function without centralized control to maintain resilience against single points of failure [29].

3. Adaptive Security Frameworks for Packet Dropping Attacks

3.1 Trust-Based Detection and Mitigation

Khan et al. [30] proposed TASRP (Trust Aware Secure Routing Protocol) has both direct and indirect trust assessment features. A node overhears its neighbors' forwarding activities and calculates direct trust scores that are shared with adjacent nodes. Those trust values are weighted differently based on their historic behavior, suspicious nodes are filtered out from the routing. Arisdakessian et al. [31] TRPM (Trust based RPL with Packet Marking) modifies the trust model with packet marking. Each forwarding node marks packets with a trivial signature, which serves as evidence that can be used for finding dropping nodes. System modifies trust threshold values based on the actual conditions of the network, which leads to improved security as well as performance. Altaf et al. [32] DTRAB (Dynamic Trust and Recommendation-based Adaptive Blacklisting) enables time sensitivity in trust judgements. Recently observed behavior is given greater significance than the older ones, giving the system flexibility in combating suddenly malicious-turned nodes. DTRAB applies a sliding window method for trust evaluation where the size of the window is dependent on the stability of the network.

3.2 Game Theory-Based Approaches

Legitimate nodes and attackers in a network interaction can be described using a game-theoretical frameworks that derive optimal defense solutions.

GTMS (Game Theory-based Multi-path Routing Strategy) developed by Sheu et al. [33], describes packet routing as a non-cooperative game in which nodes compete to decide the forwarded paths to maximize packet delivery and minimize resource use. The system modifies its strategy according to learned attack behavior, such as increasing redundancy of paths when dropping of packets is detected. Wu et al., [34] introduced ABRT (Adaptive Bayesian Reputation-based Trust) that uses game theory along with Bayesian statistics to determine optimal inspection rates. The framework treats the inspection-dropping problem as a Bayesian game and calculates how often nodes should be looked at depending on a threat level, thus saving energy, but at the same time ensuring security.

3.3 Machine Learning-Based Detection

Machine learning methods can capture more subtle patterns of behavior likely associated with packet drops which may be missed by rules. Shao et al. [35] proposed MLAD (Machine Learning Anomaly Detection) that uses supervised learning to classify nodes as benign or hostile based on analyzed network traffic features. The model self-adjusts its classification models by periodically retraining with new data, thus improving as techniques for attack change. Attique et al. [36] proposed FDML (Fog-assisted Distributed Machine Learning) which shifts part of the computation of machine learning to fog nodes.This approach uses ensemble techniques that integrate several lightweight models, each

tailored for spotting specific dropping actions. The model's weight in the system is adjusted depending on how the model performed in the most recent detection. Ahmadi et al. DLAD (Deep Learning-based Routing Anomaly Detection), 37, uses deep neural networks to automatically learn sophisticated dropping behavior without an explicit feature engineering process. It attempts to transfer learned models to new network environments and lowers the training information needed, while still being able to detect features accurately. The table 1 is the comparative analysis of three main strategies of reducing packet dropping attacks in IoT networks.

Table 1: Comparative analysis of the three main approaches to mitigating packet dropping attacks in IoT networks

Framework Approach	Key Strengths	Key Limitations	Implementation Complexity	Resource Requirements	Adaptability
Trust-Based Detection and Mitigation	• Intuitive conceptual model • Lightweight implementation options • Effective against consistent attackers • Can operate in distributed environments	• Vulnerable to on-off attacks • Cold start problem (initial trust values) • Trust propagation challenges • Limited contextual awareness	Medium	Low to Medium	Medium
Game Theory-Based Approaches	• Models' attacker-defender dynamics • Finds optimal inspection strategies • Can predict attacker behavior • Strong theoretical foundation	• Requires accurate utility functions • Assumes rational adversaries • Computationally intensive for complex games • Often requires centralized control	High	Medium to High	High
Machine Learning-Based Detection	• Can identify subtle attack patterns • Adapts to evolving threats • High detection accuracy • • Minimal domain knowledge required	• Training data requirements • Black-box decision making • Computational overhead • Vulnerability to adversarial samples	High	High	Very High

Some of the most advanced security architectures combine features from several different approaches' perspectives. Trust models enhanced with machine learning for better trust value estimation, game-theoretic optimization of inspection strategies with trust values as input, federated learning for resource-constrained devices, and hybrid systems that adaptively switch among several detection approaches depending on the network state and devices' capabilities. These multi-faceted frameworks would be able to address the shortcomings of each single method while taking advantage of their interdependencies to safeguard IoT ecosystems against highly adaptive packet dropping attacks.

4. Security Frameworks for Modification and Manipulation Attacks

4.1 Cryptographic Approaches

The vast majority of modifications IoT routing attacks are mitigated using various cryptographic techniques. These methods often underpin the solution. SARP (Secure Adaptive RPL Protocol) by Vishal et al., [38] secures the control messages of the routing protocol using lightweight symmetric

key cryptography. This protocol implements dynamic key management whereby refreshing of keys takes place periodically depending on the level of activity in the network and the pattern of threats in the vicinity. SARP, Secure Adaptive RPL Protocol, mitigated the resource constraints by flexibly and adaptively changing the strength of the applied cryptographic primitives to the level of criticality of the data being protected. Bhasin et al. [39] integrated cryptographic validation with path redundancy and proposed a novel TRAIL (Trust-aware Routing with Integrated Authentication for Low-power networks) system. The system employs hash chains for message authentication and routing and increase the cryptographic overhead in hostile operational environments. Critical control messages receive strong verification, while non-critical routine updates receive simple verification in TRAIL's selective message authentication scheme.

4.2 Secure Routing Modules

A number of frameworks include specific security modules, which can be associated with traditional routing protocols. Sahraoui et a1 SRMP (Secure Routing Module Protocol) [40]. developed a security module for RPL that provides a security plug-in layer to check the authenticity of routing information. The module dynamically determines verification procedures depending on device capability and general network environment, applying more robust protection to critical infrastructure backbone nodes and less to leaf nodes. Alaoui et al. [41] developed MARS (Modular Adaptive Routing Security), which aims at decomposing the routing logic and security functionality. This design allows the system to replace security components without discontinuing routing processes, thus coping with new security challenges posed by the dynamic network environment. MARS uses context adaptive security, which determines the appropriate level of protection depending on the state of the security of the network. The comparative analysis of the three most principal methods in dealing with overriding and falsification attacks of IoT routing protocols is given in Table 2.

Table 2: Comparative analysis of the three main approaches to addressing modification and manipulation attacks in IoT routing protocols

Framework Approach	Key Strengths	Key Limitations	Implementation Complexity	Resource Requirements	Scalability
Cryptographic Approaches	• Strong mathematical security guarantees• Mature, well-tested methods • Direct protection of data integrity • Relatively straightforward implementation	• Key management challenges • Computational overhead for constrained devices • Energy consumption concerns • Trade-off between security and performance	Medium	Medium	Medium
Secure Routing Modules	• Modular integration with existing protocols • Separation of routing and security concerns • Adaptable security levels based on context • Backward compatibility potential	• Possible integration inconsistencies • Protocol overhead • Implementation complexity across heterogeneous devices • Standardization challenges	Medium to High	Low to Medium	High
Blockchain-Based Solutions	• Immutable record of routing information • Distributed trust model • Resistant to single-point failures	• Significant computational overhead • Transaction latency issues • Storage requirements	Very High	High	Low to Medium

	• Transparent verification mechanism	• Consensus energy costs			

4.3 Blockchain-Based Solutions

The implementation of blockchain technologies provides great methods for protecting the immutability of routing information. Saikumari's (42) BC-RPL utilized blockchain technology for securely storing state changes of routing information. The system implements a lightweight consensus designed for lower performing devices that has adaptive difficulty relative to the existing threat level. Critical routing information such as rank information is stored on-chain while less important data is stored off-chain. Zhu et al. (43) developed DLBSR, which is short for Distributed Ledger Based Secure Routing, and proposes the use of a permissioned blockchain for tracking routing changes within IoT networks. The system balances performance and security by dynamically modifying the rate of blockchain commits relative to network stability and detected anomalies.

5. Packet Classification Systems for DoS Attack Mitigation

5.1 Traffic Analysis and Classification

The windshield to effective DoS mitigation is being able to tell the difference between legitimate and malicious traffic patterns. Gang et al. [44] and his team proposed a TLPC (Two-Level Packet Classification) technique which employs a hierarchical classification approach. The first level utilizes lightweight statistical analysis to detect suspicious traffic and the second level sophisticated algorithms to confirmed anomalies. The system adaptively adjusts detection thresholds based on historical traffic patterns and current network traffic. Salman et al. [45] created MLPC (Machine Learning-based Packet Classification) which uses a combination of distinct classification algorithms for different DoS attack signatures. The framework incorporates adaptive feature selection in with the observed attack patterns and thus optimizes the computation with maintained detection.

5.2 Distributed Detection and Mitigation

Alhasawi et al. [46] proposed COID (Collaborative IoT Defense) where devices under the umbrella of IoT collaborate to mitigate attacks from rogue IoT devices. Intelligent nodes learn and share threat information by utilizing federated learning. The system suffers from poor false positive rate due to dependency on the consensus coming from participating devices. Bostani and Yilmaz [47] advanced the technology with proposed DDMD (Distributed Detection and Mitigation of DoS) that further refines detection workload distribution according to device capability.The system uses role-oriented packet inspection in which powerful nodes carry out complicated analysis while resource-constrained devices focus on simple checks. DDMD shifts detection workloads adaptively depending on the existing energy and processing capacity.

5.3 Software-Defined Networking Approaches

With the SDN approach, it is possible to provide centralized control for the execution of dynamic defense mechanisms. Saba et al. [48] proposed SDNIDS (SDN-based Intrusion Detection System) that uses the visibility provided by SDN controllers to detect coordinated DoS attacks that may go unnoticed locally. The system builds flow rules that enable the redirection of suspicious traffic for detailed inspection while maintaining an optimal balance between network performance and security objectives. Zhang et al. [49] developed deep reinforcement learning-based vulnerability-aware network adaptations for resilient networks. This combines SDN and Network Function Virtualization (NFV) to facilitate dynamic deployment of DoS countermeasures. In these attack scenarios, the framework allocates essential computational resources to critical network functions to ensure service

continuity during an attack. Table 3 shows the comparison of the three principal methods for Classifying packets in IoT networks and mitigating DoS attacks.

6. Integrated Frameworks and Future Directions

6.1 Comprehensive Security Architectures

Current studies have concentrated on creating composite architectures capable of handling different attack vectors at once. Kait et al.'s FORTRESS (Flexible ORganized Trusted Routing and Efficient Security System) [50] combines trust-based routing with cryptographic validation and traffic filtering through a layered security architecture. The system implements adaptive security policies that alter levels of protection according to contextual parameters such as device position, the data's level of sensitivity, and previously identified threat patterns. Zhou et al. [51] put forward Secure Hierarchical IoT Defense, which utilizes several complementary security mechanisms to implement deeper layers of defense, or defense-in-depth. The framework uses context-aware adaptation whereby security measures change automatically depending on the state of the network, how critical the mission is, and anomally detection.

Table 3: Comparative analysis of the three main approaches to DoS attack mitigation through packet classification in IoT networks

Framework Approach	Key Strengths	Key Limitations	Implementation Complexity	Resource Requirements	Real-time Performance
Traffic Analysis and Classification	• Detailed inspection of packet characteristics • Ability to detect sophisticated attack signatures • Adaptable detection thresholds • Can distinguish legitimate from malicious traffic	• Computationally intensive deep packet inspection • Potential for false positives • Limited view of coordinated attacks • Challenge of encrypted traffic analysis	Medium	Medium to High	Medium
Distributed Detection and Mitigation	• Collaborative intelligence across devices • Load distribution across network • Resilience against distributed attacks • Reduced false positives through consensus	• Communication overhead for threat intelligence • Coordination challenges • Risk of compromised detection nodes • Complex implementation in heterogeneous networks	High	Low to Medium	High
Software-Defined Networking Approaches	• Centralized control and visibility • Dynamic reconfiguration capabilities • Flexible traffic steering and filtering • Resource allocation based on attack	• SDN controller as single point of failure • Control plane overhead • Implementation complexity • Compatibility issues with legacy devices	Very High	Medium	Very High

	conditions				

6.2 Artificial Intelligence for Adaptive Security

Dynamic capabilities of AI present an opportunity for creating actually adaptive security controls. AISA (Artificial Intelligence for Security Adaptation) by Zaman et al. [52] uses reinforcement learning to improve future responses to changing threat environments by optimizing security configuration changes over time. The system treats the problem of securing system changes as a Markov Decision Process and develops policies that minimize the resource cost of security relative to the strength of the defense deployed. Rashid et al. [53] introduced Federated Artificial Intelligence which applies federated learning to the distribution of sensitive data which is necessary to train anomaly detection models in different deployments of IoT devices.Even for severely resource-constrained devices, the framework guarantees effective protection by adaptively modifying local model complexity in accordance with the capability of the device.

6.3 Research Challenges and Future Directions

Several challenges remain in developing fully adaptive security frameworks for IoT routing:

6.3.1 Unified Security Framework Integration

Creating truly integrated security frameworks that marry trust systems, game theory, and cryptographic and machine learning approaches is still an open problem. Existing methods often focus on one or several attack vectors in isolation, and therefore leave gaps in security at the interfaces of different protection mechanisms. Research is still needed to develop overarching frameworks that can integrate multiple defense strategies and still maintain a coherent security stance. That level of integration has to happen without incurring excessive cost or creating new attack surfaces at the boundaries of different security components [54].

6.3.2 Cost-Effective Security For Ultra Resource Dependent Devices

With the increasing adoption of IoTs comes the incorporation of even more resource constrained devices, making the balance between security and practicality much more difficult to manage. A lot of edge devices, especially those deployed for long periods of time without maintenance access transform into ‘forgotten’ devices, which make many memory footprints, energy budgets, or computational capacity approaches impractical. Research needs to move in the direction of ultra-lightweight security primitives capable of providing practical protection with virtually no resource usage, possibly with the aid of hardware built for security accelerators or new forms of cryptography for severely limited open spaces [55].

6.3.3 Adapting Response Mechanisms

Evening this up, my advanced security frameworks whose reaction is overly simplistic with the way that computer systems evolves its needs and caters to the growing threats. It often seems as if the systems of the future seek to implement multi-dimensional and context-based responsive systems that instantaneously reorganize the level of protection based on the attack patterns, the state of the network, and mission importance. This type of capability should not be partitioned beyond threshold-based alterations alone to come with modifying entire defence strategies at an intricate level including learning based on the changes on the threats and all the means operated in need and based on the constrain of tasks and the derived objectives to set the security systems and the defence structures in a normalized wide range of emergent constraints consideration [56].

6.3.4 Coordination Across Layers of Security

The implemented security measures should potentially distributed their operation within defined limits of certain protocol classes so that there is advanced possibility of abuse in the attack at the sub classes boundaries. Complex systems have to be designed and constructed which are able to offer unity for the actions of both illegal and legal perception at and above the physical, data link, network and application layers. It is advisable for further inquiries of HID interfaces to the complex systems to bundle the provided security within specific, informal and other high level of system architecture modularity constructions or informal protections in the entire internet of things. Such captures must expose advanced cover set and practically exploitable on nature's heterogeneous IoT world [57].

6.3.4 Privacy-Preserving Collaborative Defense

Modern collaborative defense strategies partition security measures between different entities, which aids in harnessing resources. However, such strategies introduce new hurdles in the form of privacy breaches particularly when security telemetry data and traffic patterns are concerned. This emphasizes the need to automate proactive sensitive information control systems that allow collaborative defense operations to capture and mitigate threats in a sensitive information safeguarded environment. Such efforts are achievable through a secured multi-party computation environment, differential privacy, and federated learning that do not compromise on detection performance while censoring sensitive information [58].

6.3.5 Formal Verification and Security Guarantees

The advanced adaptability in a modern security framework makes its verification for correctness under a specific set of conditions more difficult to determine. Future work should pay attention towards building formal verification techniques for adaptive security systems capable of proving the provision of some predefined level of protection and some immunity from a range of attacks. These methods must cope with security being inherently uncertain due to system mobility while still providing meaningful security guarantees, maybe using probabilistic methods of verification or reasoning about system security properties in a compositional manner.

7. Conclusion

This survey has analyzed adaptive security frameworks concerning IoT routing protocols, concentrating on the packet dropping, modification, and denial of service countermeasures. Based on the current analysis, there seems to be an increase in composite defenses augmented with artificial intelligence for post deployment modification. Trust-based systems have proven useful in containing the packet dropping attacks when they are integrated with some machine learning behavior analysis techniques. For modification attacks, lightweight cryptographic methods are still fundamental, although blockchain based approaches are emerging for assuring the integrity of the routing information. DoS attacks are increasingly being dealt with through a combination of distributed intelligent detection and centralized intelligence, which is mostly done using SDN technologies.

In the coming years, research attempts will be necessary in order to design truly comprehensive frameworks for multi attack vector with an emphasis on adaptability to new threats. Such frameworks will have to meet the necessary target of balancing security provision with the available resources that are characteristic of the IoT environment and therefore need situation aware protection adaptation. The efforts of implementing the Internet of Things (IoT) into core infrastructure and sensitive areas market the need of not only robust, but responsive security mechanisms for the routing protocols as a prime area of research towards practical solution.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, 2015.

[2] Statista Research Department, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025," Statista, 2021.

[3] E. Bertino and N. Islam, "Botnets and Internet of Things Security," Computer, vol. 50, no. 2, pp. 76-79, 2017.

[4] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, "IoT Security: Ongoing Challenges and Research Opportunities," IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230-234, 2014.

[5] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483-2495, 2018.

[6] S. Mohammadi and H. Jadidoleslamy, "A Comparison of Physical Attacks on Wireless Sensor Networks," International Journal of Peer to Peer Networks, vol. 2, no. 2, pp. 24-42, 2011.

[7] L. Wallgren, S. Raza, and T. Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things," International Journal of Distributed Sensor Networks, vol. 9, no. 8, 2013.

[8] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," Computer, vol. 50, no. 7, pp. 80-84, 2017.

[9] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142, 2017.

[10] Winter, Tim, Pascal Thubert, Anders Brandt, Jonathan Hui, Richard Kelsey, Philip Levis, Kris Pister, Rene Struik, Jean-Philippe Vasseur, and Roger Alexander. *RPL: IPv6 routing protocol for low-power and lossy networks*. No. rfc6550. 2012.

[11] K. Kim, S. D. Park, G. Montenegro, S. Yoo, and N. Kushalnagar, "6LoWPAN Ad Hoc On-Demand Distance Vector Routing (LOAD)," IETF Internet Draft, 2007.

[12] T. Clausen, A. C. de Verdiere, J. Yi, A. Niktash, Y. Igarashi, H. Satoh, U. Herberg, C. Lavenu, T. Lys, and J. Dean, "The Lightweight On-demand Ad hoc Distance-vector Routing Protocol - Next Generation (LOADng)," IETF Internet Draft, 2016.

[13] O. Gaddour, A. Koubâa, and M. Abid, "Quality-of-service aware routing for static and mobile IPv6-based low-power and lossy sensor networks using RPL," Ad Hoc Networks, vol. 33, pp. 233-256, 2015.

[14] S. Dokurer, Y. M. Erten, and C. E. Acar, "Performance Analysis of Ad-hoc Networks under Black Hole Attacks," Proceedings of the IEEE SoutheastCon, pp. 148-153, 2007.

[15] S. Biswas, T. Nag, and S. Neogy, "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET," IEEE International Conference on Applications and Innovations in Mobile Computing, pp. 157-164, 2014.

[16] I. Khalil, S. Bagchi, and N. B. Shroff, "LITEWORP: Detection and isolation of the wormhole attack in static multihop wireless networks," Computer Networks, vol. 51, no. 13, pp. 3750-3772, 2007.

[17] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: analysis &defenses," Proceedings of the 3rd international symposium on Information processing in sensor networks, pp. 259-268, 2004.

[18] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," IEEE INFOCOM 2003, vol. 3, pp. 1976-1986, 2003.

[19] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8, no. 5, pp. 521-534, 2002.

[20] A. Mayzaud, R. Badonnel, and I. Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things," International Journal of Network Security, vol. 18, no. 3, pp. 459-473, 2016.

[21] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," International Journal of Computer Applications, vol. 111, no. 7, pp. 1-6, 2015.

[22] C. Pu, "Sybil Attack in RPL-Based Internet of Things: Analysis and Defenses," IEEE Internet of Things Journal, vol. 7, no. 6, pp. 4937-4949, 2020.

[23] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, pp. 46-57, 2005.

[24] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "A study of RPL DODAG version attacks," IFIP International Conference on Autonomous Infrastructure, Management and Security, pp. 92-104, 2014.

[25] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," IEEE Wireless Communications and Networking Conference, pp. 2728-2733, 2014.

[26] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266-2279, 2013.

[27] O. Garcia-Morchon, S. Kumar, and M. Sethi, "Internet of Things (IoT) Security: State of the Art and Challenges," RFC 8576, 2019.

[28] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol. 76, pp. 146-164, 2015.

[29] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 618-623, 2017.

[30] Khan, Tayyab, and Karan Singh. "TASRP: a trust aware secure routing protocol for wireless sensor networks." *International Journal of Innovative Computing and Applications* 12, no. 2-3, pp.108-122, 2021

[31] Arisdakessian, Sarhad, Omar Abdel Wahab, Azzam Mourad, Hadi Otrok, and Mohsen Guizani. "A survey on IoT intrusion detection: Federated learning, game theory, social psychology, and explainable AI as future directions." *IEEE Internet of Things Journal* 10, no. 5 (2022): 4059-4092.

[32] Altaf, Ayesha, Haider Abbas, Faiza Iqbal, Malik Muhammad Zaki Murtaza Khan, Abdul Rauf, and Tehsin Kanwal. "Mitigating service-oriented attacks using context-based trust for smart cities in IoT networks." *Journal of Systems Architecture* 115 pp.102028, 2021.

[33] J. P. Sheu, C. X. Hsu, and C. Ma, “A Game Theory Based CongestionControl Protocol for Wireless Personal Area Networks,” in Proceedings of 39th Annual Computer Software and Applications Conference(COMPSAC), vol. 2, July 2015.

[34] Wu, Yingzhen, and Yan Huo. "Cross-layer secure transmission schemes for social internet of things: Overview, opportunities and challenges." *Neurocomputing* 500 (2022): 703-711.

[35] Shao, Pengyan, and Tongwei Lu. "MLAD: Manifest and latent anomaly detection based on the integration of reconstruction and MLFP-KNN methods." *Measurement Science and Technology* 36, no. 1, pp.015431, 2024.

[36] Attique, Danish, Hao Wang, and Ping Wang. "Fog-assisted deep-learning-empowered intrusion detection system for RPL-based resource-constrained smart industries." *Sensors* 22, no. 23, pp.9416, 2022.

[37] Ahmadi, Khatereh, and Reza Javidan. "A Trust Based Anomaly Detection Scheme Using a Hybrid Deep Learning Model for IoT Routing Attacks Mitigation." *IET Information Security* 2024, no. 1 pp. 4449798, 2024.

[38] Vishal Sharad, Hingmire, Santosh R. Desai, and Kanse Yuvraj Krishnrao. "SAOA: Multi-Objective Fault-Tolerance Based Optimized RPL Routing Protocol in Internet of Things." *Cybernetics and Systems* 55, no. 8 pp.2118-2139, 2024.

[39] Bhasin, Vandana, Sushil Kumar, Prem Chandra Saxena, and Chittaranjan Padmanabha Katti. "Trust-Aware Distributed and Adaptive Energy Efficient Secure Routing in Sensor Networks." *Ad Hoc Sens. Wirel. Networks* 50, no. 1-4 pp.73-115, 2021.

[40] Sahraoui, Somia, and Nabil Henni. "SAMP-RPL: secure and adaptive multipath RPL for enhanced security and reliability in heterogeneous IoT-connected low power and lossy networks." *Journal of Ambient Intelligence and Humanized Computing* 14, no. 1 pp.409-429, 2023.

[41] El Alaoui, Sara, and Byrav Ramamurthy. "MARS: A multi-attribute routing and scheduling algorithm for DTN interplanetary networks." *IEEE/ACM Transactions on Networking* 28, no. 5 pp.2065-2076, 2020.

[42] Saikumari, Thakur, and George Victo Sudha. "An improved congestion handling in blockchain secured cloud based healthcare system." International Journal of Intelligent Engineering & Systems 17, no. 2, 2024.

[43] Zhu, Qingyi, Seng W. Loke, Rolando Trujillo-Rasua, Frank Jiang, and Yong Xiang. "Applications of distributed ledger technologies to the internet of things: A survey." *ACM computing surveys (CSUR)* 52, no. 6 pp.1-34, 2019.

[44] Gang, Qiao, Wazir Ur Rahman, Feng Zhou, Muhammad Bilal, Wasiq Ali, Sajid Ullah Khan, and Muhammad Ilyas Khattak. "A Q-Learning-Based Approach to Design an Energy-Efficient MAC Protocol for UWSNs Through Collision Avoidance." *Electronics* 13, no., 22, pp. 4388, 2024.

[45] Salman, Ola, Imad H. Elhajj, Ayman Kayssi, and Ali Chehab. "A review on machine learning–based approaches for Internet traffic classification." *Annals of Telecommunications* 75, no. 11, pp. 673-710, 2020.

[46] Alhasawi, Yaser, and Salem Alghamdi. "Federated learning for decentralized DDoS attack detection in IoT networks." IEEE Access 12, pp. 42357-42368, 2024.

[47] Yilmaz, Yasin, and Suleyman Uludag. "Mitigating IoT-based cyberattacks on the smart grid." In *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pp. 517-522. IEEE, 2017.

[48] Saba, Tanzila, Amjad Rehman, Tariq Sadad, Hoshang Kolivand, and Saeed Ali Bahaj. "Anomaly-based intrusion detection system for IoT networks through deep learning model." *Computers and Electrical Engineering* 99, pp.107810, 2022.

[49] Zhang, Qisheng, Jin-Hee Cho, Terrence J. Moore, and Frederica Free Nelson. "DREVAN: deep reinforcement learning-based vulnerability-aware network adaptations for resilient networks." In *2021 IEEE Conference on Communications and Network Security (CNS)*, pp. 137-145. IEEE, 2021.

[50] Kait, Ramesh, Sarbjit Kaur, Purushottam Sharma, Chhikara Ankita, Tajinder Kumar, and Xiaochun Cheng. "Fuzzy logic-based trusted routing protocol using vehicular cloud networks for smart cities." *Expert Systems* 42, no. 1 e13561, 2025.

[51] Zhou, Xiaokang, Wei Liang, Weimin Li, Ke Yan, Shohei Shimizu, and Kevin I-Kai Wang. "Hierarchical adversarial attacks against graph-neural-network-based IoT network intrusion detection system." *IEEE Internet of Things Journal* 9, no. 12,pp.9310-9319, 2021.

[52] Zaman, Shakila, Khaled Alhazmi, Mohammed A. Aseeri, Muhammad Raisuddin Ahmed, Risala Tasin Khan, M. Shamim Kaiser, and Mufti Mahmud. "Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey." *Ieee Access* 9, pp. 94668-94690, 2021.

[53] Rashid, Md Mamunur, Shahriar Usman Khan, Fariha Eusufzai, Md Azharuddin Redwan, Saifur Rahman Sabuj, and Mahmoud Elsharief. "A federated learning-based approach for improving intrusion detection in industrial internet of things networks." *Network* 3, no. 1,pp.158-179, 2023.

[54] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Systematically Evaluating Security and Privacy for Consumer IoT Devices," Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, pp. 1-6, 2017.

[55] T. Chothia, F. D. Garcia, C. Heppel, and C. M. A. Stone, "Why Banker Bob (Still) Can't Get TLS Right: A Security Analysis of TLS in Leading UK Banking Apps," Financial Cryptography and Data Security, pp. 579-597, 2017.

[56] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov, and A. V. Vasilakos, "The Quest for Privacy in the Internet of Things," IEEE Cloud Computing, vol. 3, no. 2, pp. 36-45, 2016.

[57] O. Garcia-Morchon, S. Kumar, and M. Sethi, "Internet of Things (IoT) Security: State of the Art and Challenges," RFC 8576, 2019.

[58] Lou, David, Jan Holler, Dhruvin Patel, Ulrich Graf, and Matthew Gillmore. "The industrial internet of things networking framework." *Industrial IoT Consortium*, 2021