Detection of DDoS Cyberattack Using a Hybrid Trust-Based Technique for Smart Home Networks

Oghenetejiri Okporokpo, Funminiyi Olajide, Nemitari Ajienka, Xiaoqi Ma
Department of Computer Science, Nottingham Trent University, Clifton Lane, Nottingham NG11 8NS, United Kingdom

***Abstract*—As Smart Home Internet of Things (SHIoT) continue to evolve, improving connectivity and security whilst offering convenience, ease, and efficiency is crucial. SHIoT networks are vulnerable to several cyberattacks, including Distributed Denial of Service (DDoS) attacks. The ever-changing landscape of Smart Home IoT threats presents many problems for current cybersecurity techniques. In response, we propose a hybrid Trust-based approach for DDoS attack detection and mitigation. Our proposed technique incorporates adaptive mechanisms and trust evaluation models to monitor device behaviour and identify malicious nodes dynamically. By leveraging real-time threat detection and secure routing protocols, the proposed trust-based mechanism ensures uninterrupted communication and minimizes the attack surface. Additionally, energy-efficient techniques are employed to safeguard communication without overburdening resource-constrained SHIoT devices. To evaluate the effectiveness of the proposed technique in efficiently detecting and mitigating DDoS attacks, we conducted several simulation experiments and compared the performance of the approach with other existing DDoS detection mechanisms. The results showed notable improvements in terms of energy efficiency, improved system resilience and enhanced computations. Our solution offers a targeted approach to securing Smart Home IoT environments against evolving cyber threats.**

***Keywords*—Trust; smart home; IoT; DDoS; denial of service; DoS; cyber threats; techniques**

I. Introduction

Over the past few years, the advancement of Internet of Things (IoT) technology has resulted in ease of integration, seamless functionality and increased user satisfaction [1]. Since its inception, we have witnessed an increase in the number of smart home Internet of Things (SHIoT) devices such as smart bulbs, smart TVs, smart alarms, smart refrigerators, and smart fans [2] These have in turn resulted in diverse applications such as smart cities [3], smart grid systems [4], and smart healthcare systems [5].

However, security remains a paramount concern. specifically in smart home network environments, which usually encompass, wireless and mobile ad hoc networks. These environments generally deviate from traditional wired networks, boasting distinctive attributes such as shared resources, node mobility, and limited transmission range [6]. As a result of the generally limited processing power of mobile nodes in smart home networks, security techniques that have proven successful in wired networks tend to fail in wireless networks [7]. Furthermore, because nodes in smart home networks are free to join or leave, their dynamic nature causes network topologies to change quickly, which makes maintaining network security extremely difficult. The creation of complex yet effective security measures suited to these environments is necessary [8].

In our work, we explore the escalating cybersecurity threats faced by Smart Home Internet of Things (SHIoT) networks, particularly focusing on Distributed Denial of Service (DDoS) attacks. Traditional security measures have proven inadequate in safeguarding these networks, requiring innovative solutions.

The contribution of this research is a proposed novel Trust-based DDoS attack detection model tailored specifically for SHIoT environments. Through comprehensive analysis, the paper identifies prevalent DDoS attack types targeting these networks, delving into their unique characteristics and implications. It evaluates the effectiveness of current cybersecurity measures and introduces a trust-based mitigation technique designed to counter each identified attack vector. By emphasizing the significance of trust-based approaches, the research not only contributes to the enhancement of cybersecurity in smart home settings but also identifies key avenues for future exploration. This study lays the groundwork for more resilient and secure smart home networks, ensuring the confidentiality and integrity of IoT communications amidst the evolving landscape of cyber threats.

The results show that the proposed technique can effectively improve the security of smart homes and enhance the efficiency of smart home network environments. The key contributions of our work are summarized as follows:

- The proposed approach incorporates Knowledge-based trust computations, resulting in more efficient and effective trust aggregations in smart homes.
- Observational-based Trust optimization is used to update trust and reputation, allowing for the system to draw upon the shared encounters of its neighbouring nodes or devices on the network which allows the network parameters to be adjusted as needed.
- The proposed technique deploys a hybrid trust-based technique for trust propagation, trust updation and trust formation which classifies malicious nodes using knowledge, reputation, and observational experience, resulting in better identification and mitigation of security threats in smart homes.

The layout of the paper is as follows. In Section II, we discuss the related work. In Section III, we describe our methodology for trust in smart home network environments. Section IV describes in detail our proposed trust-based system while in Section V. We evaluate the system performance within

smart home networks. In Section VI future research directions are highlighted.

II. Related Work

In recent years, the field of SHIoT security has gained significant attention from researchers, because of the peculiar vulnerabilities of these SHIoT devices [9]-[12]. A smart home is an essential component of intelligent computing, by easily integrating with home devices to control and monitor their operations. It often uses cloud computing for storage and scalable processing power. Smart home appliances can now be remotely controlled from any location thanks to cloud computing [13]. Smart homes improve convenience, security, and energy efficiency by allowing users to effectively manage gadgets. These gadgets offer a great deal of convenience in addition to time, money, and energy savings. The main control interface for the smart home system is usually a smartphone or tablet. In this section, we review the existing literature covering key SHIoT security challenges, the nature of DDoS attacks on SHIoT networks, and existing cybersecurity solutions.

A. Overview of SHIoT Security Challenges

The ubiquitous nature of SHIoT creates some unique weaknesses and challenges which are inherent in their design. Almost any device can be equipped with the necessary technology to facilitate data transmission between IoT devices and their connected networks. Each node in a SHIoT network generally operates under energy constraints, creating an incentive for nodes to selfishly conserve their resources [14]. This self-preserving behaviour can negatively impact the overall functionality and efficiency of the network. Another unique challenge is due to their typical deployment in unattended and often hostile environments meaning that these networks often rely on thousands of low-cost sensors to monitor even small areas, which necessitates producing sensors at minimal cost. This cost reduction compromises the tamper-resistant properties of the SHIoT devices. SHIoTs are typically vulnerable to physical capture by adversaries [15]. Ensuring secure and efficient operation is challenging due to these factors particularly when threats like Distributed Denial of Service (DDoS) attacks target these SHIoT networks. One of the main concerns in smart homes is unauthorized access, where sensitive user data, such as video feeds or personal preferences can be intercepted if devices do not have proper access control protocols in place [16]. Due to the computational limitations of SHIoT devices, there are limits on the implementation of advanced cryptographic algorithms, thereby leading to exposure to various types of cyberattacks.

Existing security models oftentimes focus on traditional IT systems, overlooking IoT's resource limitations and real-time processing needs [8]. The lack of standardized security practices across IoT device manufacturers exacerbates these issues, leaving devices vulnerable to exploitation and making it challenging to implement uniform security measures across diverse IoT ecosystems.

B. DDoS Attacks

DDoS attacks have become increasingly common in SHIoT networks, largely due to the massive deployment of SHIoT devices, which can be easily exploited due to weak security configurations [17]. Common DDoS attacks within the SHIoT environment include HTTP floods, UDP floods, and TCP SYN floods.

1) HTTP Flood attacks: HTTP flood attacks are one of the most common DDoS cyberattacks. These attacks are carried out by inundating the victim with a massive number of HTTP connection requests. These attacks aim to overwhelm the target server's resources and prevent legitimate traffic from accessing the server. In the context of IoT, HTTP floods can target cloud-based services associated with smart home devices, causing network slowdowns and disruptions [18]. Researchers Marleau et al. proposed an HTTP flood detection and mitigation technique for Software-defined networks (SDN) using Network Ingress Filtering [19].

2) UDP Flood attacks: UDP flood attacks flood the victim network or device with many User Datagram Protocol (UDP) packets. The extensive volume of packets inundates the target server, aiming to overwhelm its processing and response capabilities. UDP floods are particularly disruptive in SHIoT environments, where devices rely on minimal bandwidth and have limited packet-processing capabilities [20]. An example is the DNS amplification attack, where the attacker spoofs the source IP address of the victim and sends a small request to the DNS server. The DNS server replies with large responses, affecting the victim's performance. Researchers Lee et al. [21] proposed the use of specific IPtables rules and Linux-based firewall utilities, to mitigate UDP flood attacks.

3) TCP SYN Flood attacks: This type of attack exploits the TCP handshake mechanism by sending repeated SYN requests, but failing to respond to SYN-ACK replies, leaving the connection half-open. This can consume server resources and result in denial of service. Smart home devices, which often operate on simple network architectures, are vulnerable to these types of connection-based floods [22]. Bensaid et al. proposed a fog computing-based SYN Flood DDoS attack mitigation technique which uses an adaptive neuro-fuzzy inference system (ANFIS) and SDN assistance [23].

The impact of these attacks on SHIoT networks is significant, leading to degraded performance, reduced availability, and even complete network outages. DDoS attacks also open pathways for further malicious activities, such as data breaches or malware infiltration, by exploiting compromised devices within the IoT network [24].

C. Existing DDoS Mitigation Solutions

Current DDoS mitigation techniques include solutions like rate limiting, firewalls, and anomaly detection. However, while these methods offer some level of protection, they are often insufficient or computationally demanding for IoT environments:

1) Rate limiting: This approach restricts the number of requests allowed per unit of time, which can mitigate DDoS attacks. However, IoT devices may still be overwhelmed by legitimate traffic, and rate limiting does not effectively distinguish between malicious and legitimate requests [25].

2) Firewalls: Traditional firewalls monitor all incoming traffic attempting to enter a network and can block unwanted traffic. However, they are often unsuitable for IoT devices due to their processing and memory limitations. Additionally, firewalls require frequent updates to stay effective, which may not be feasible for resource-constrained SHIoT devices [26].

3) Anomaly detection: Anomaly detection, also known as behavioural detection, involves identifying predefined signatures or events that deviate from normal system behaviour. These systems use methods such as machine learning and analysis to identify abnormal patterns of network traffic [27]. While effective, these systems are computationally intensive, requiring processing power that most SHIoT devices lack. Moreover, the high rate of false positives in anomaly detection can lead to unnecessary slow-down in network performance, impacting the reliability of IoT services [28].

These traditional solutions, while useful in general networking environments, fall short of providing scalable, efficient, and reliable security for SHIoT networks, particularly when faced with DDoS attacks in smart home environments.

D. Trust-Based Security Approaches

As a result of the limitations of other DDoS mitigation techniques, researchers have explored trust-based security models tailored to various technologies. Trust-based security mechanisms aim to establish a level of trust for each device or network node based on behaviour, interaction history, and reputation, allowing the network to isolate untrustworthy devices or nodes in real time.

Several studies have highlighted the benefits of trust-based approaches in distributed and resource-constrained environments like IoT [29]-[31]. Trust-based models can effectively mitigate insider threats by flagging devices that exhibit suspicious behaviour, such as attempting excessive communication or participating in botnet-like activities [21]. Trust-based systems are also adaptable, requiring less processing power than anomaly detection making them suitable for IoT devices with limited computational capacity [32].

Shuhaiber and Mashal [33] presented a multilayered trust-based technique within IoT ecosystems, offering a theoretical insight into the intricate relationships between Trust Stance, and their impact on trust dynamics within IoT networks. Khatereh et al. [34] introduced a trust management model for anomaly detection using sequence prediction and deep learning for data security in IoT networks. The proposed model provides a detection mechanism to address four RPL attacks.

Shashank et al. [35] apply a trust-based technique for reliable data packet routing in WSNs. In their approach, trust management is integrated into routing protocols, deploying the decision-making Dempster-Shafer Theory (DST) algorithm for trusted clustering and the Whale Optimization Algorithm (WOA) for routing. However, one drawback of this approach is the high energy use which is not suitable for SHIoT networks.

Adla and Ramaiah [36] propose a blockchain solution for IoT with trust management consensus. The proposed technique uses a Grey Wolf Optimization (GWO) algorithm in addition to a trust-based ensemble consensus. The trust-based ensemble consensus uses Proof of Work (PoW) and Proof of Stake (PoS) procedures to calculate trust within the network. However, one disadvantage of this approach is that the network throughput progressively drops as the number of nodes increases. Researcher Farag [37] proposed a behavioural trust-based solution to mitigate energy exhaustion attacks on the RPL protocol. The proposed protocol protects against rank attacks and Sybil attacks in IoT networks. However, the disadvantage of the technique is that the trust value is computed solely based on direct observations by each node within the network.

Researchers have proposed various methods to deal with the DDoS attacks common with IoT networks. The approaches deployed vary and authors have focused on different aspects of the security of IoT networks. It is also evident from our study on trust-based techniques and deployments that a comprehensive model incorporating all aspects of security quantification for smart home networks and services is imperative. Thus, the core focus of this research work is a proposed trust-based system as a means of securing SHIoT networks. Trust-based management techniques employ a systematic method for effectively managing and ensuring trust within the network. By incorporating trust as a core component, our model provides an adaptive, lightweight solution that enhances the security of SHIoT networks.

III. METHODOLOGY

In this section, we present the trust-based methodology that the proposed system uses to detect and mitigate Distributed Denial of Service (DDoS) attacks in SHIoT networks. The methodology is centred around a trust management system where each node in the network maintains a trust score for other nodes based on their behaviour [32]. The trust scores are dynamically updated as nodes interact with each other. When malicious behaviour is detected, such as in the case of a DDoS attack, trust scores decline, and the system can identify the compromised node and take necessary actions to mitigate the attack.

A. Network Architecture

Trust-based systems are primarily comprised of three distinct properties. Durable nodes/devices that cumulate a repository of protocols for future communication, compilation, and dissemination of information regarding ongoing communications and ensuring its availability for future reference and deployment of a propagation mechanism to aid the dissemination of trust information to peer nodes/devices on the network. Fig. 1 shows a high-level overview of the proposed Trust-based system.

Assessing the security of a smart home network is essential for any setup within the smart home environment. We've compiled a comprehensive set of security parameters crucial for gauging security within a smart home network environment.

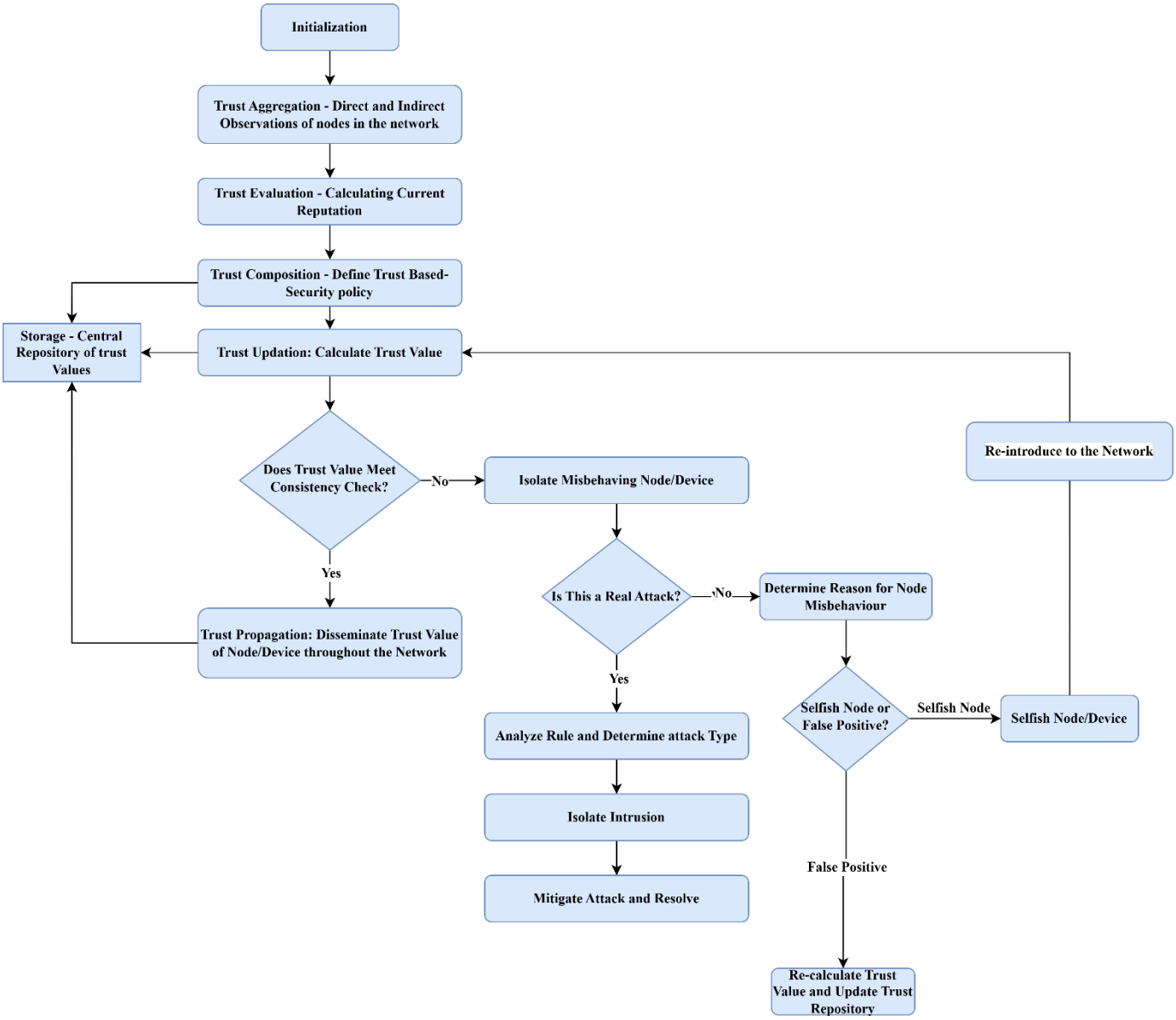

Fig. 1. High-level overview of proposed trust-based system.

These parameters form the basis of our trust model, yielding a trust value as an outcome. This trust value can either provide a holistic view of the overall security of the smart home network or can be dissected into various security aspects based on these parameters, represented as a vector.

B. Trust Definition

Trust is a measure of the reliability or reputation of a node in the network, quantifying how likely it is that a node will behave as expected, such as reliably forwarding packets without malicious intent. Trust in this context is represented as a numerical value, which is continuously evaluated and updated based on observed behaviour [30]. In the proposed system, trust is defined based on three main factors.

Packet Delivery Ratio (PDR): This measures the consistency and reliability of node y. The ratio of successfully delivered packets to the total number of packets transmitted. A high PDR implies that the node can be trusted to forward packets efficiently, whereas a low PDR may indicate the dropping or mishandling of packets, which is indicative of malicious behaviour or a selfish node trying to conserve resources.

$$PDR_{x,y}(t) = \frac{\text{Packets Delivered by node y}}{\text{Total Packets Sent to node y}} \quad (1)$$

Anomaly Detection (AD): Anomalies such as sudden traffic spikes are common indicators of a node participating in a DDoS attack. The system continuously monitors the traffic patterns, and if it detects abnormal behaviour, the anomaly detection score decreases the trust score.

$$AD_{x,y}(t) = \begin{cases} 1 & \text{if no anomaly is detected,} \\ 0 & \text{if an anomaly is detected.} \end{cases} \quad (2)$$

Response Time (RT): The time a node takes to respond to communication requests from other nodes. If the response times are consistently high (i.e., the node is unresponsive or

overloaded), this could indicate that the node is under attack or has been compromised.

$$RT_{x,y}(t) \frac{1}{\text{Observed Response Time of node y}} \quad (3)$$

C. Trust Calculation

Trust is a quantified measure based on the behaviour of nodes. Trust is evaluated based on parameters such as packet delivery ratio, response time, and anomaly detection. The trust $T_{(x,y)}(t)$ between two nodes x and y at time t is calculated as a weighted sum of the three factors mentioned above: Packet Delivery Ratio, Anomaly Detection, and Response Time. The trust calculation formula is:

$$T_{x,y}(t) = \delta \times PDR_{x,y}(t) + \theta \times AD_{x,y}(t) + \mu \times RT_{x,y}(t) \quad (4)$$

Where:

$T_{x,y}(t)$ is the trust value between nodes x and y at time t.

$PDR_{x,y}(t)$ is the packet delivery ratio between node x and node y. That is the ratio of successful packet deliveries.

$AD_{x,y}(t)$ is the anomaly detection score, indicating if node y's behaviour is deemed suspicious.

$RT_{x,y}(t)$ is the response time of node y as observed by node x. That is the delay in responses from node y.

δ, θ, μ are the weights for each factor, with $\delta + \theta + \mu = 1$, determined based on the specific requirements of the network. For example, if packet delivery is prioritized, δ would be larger.

D. Trust Update Mechanism

Trust is not static and changes as nodes interact over time. The system continuously monitors the behaviour of each node, and the trust scores are updated periodically based on recent observations. This dynamic nature ensures that the system can adapt to evolving network conditions and malicious behaviours. The trust update mechanism works as follows:

- Initial Trust Assignment: Every node starts with an initial trust value. For example, the default trust value is set to 0.5 on a scale of 0 to 1, indicating neutral trust.

$$T_{x,y}(t) = 0.5 \quad (5)$$

- Trust Evaluation: After each interaction between two nodes, the trust score is recalculated based on the Packet Delivery Ratio, Anomaly Detection, and Response Time.
- Trust Decay: Trust decays over time if no recent interaction has occurred. This decay ensures that old interactions do not overly influence current trust evaluations.

$$T_{x,y}(t+1) = (1-\omega) \times T_{x,y}(t) + \omega \times \text{new interaction data} \quad (6)$$

Where ω is a decay constant that controls how quickly trust values diminish over time.

- Threshold-Based Detection: The system sets a threshold T_{thresh} below which a node is flagged as suspicious. If the trust value $T_{(x,y)}(t)$falls below this threshold, the node is quarantined, i.e., its communication privileges are limited or monitored closely. The value of T_{thresh} is set based on network performance requirements and the acceptable level of risk.

$$\text{If } T_{x,y} < T_{thresh} \text{ then node y is flagged as suspicious.} \quad (7)$$

The value of T_{thresh} is set based on network performance requirements and the acceptable level of risk.

E. Trust Propagation in the Network

The trust scores are not only calculated on a one-to-one basis between nodes but also propagated through the network. For instance, if node x considers node y to be trustworthy, other nodes that trust x may adjust their trust values for y accordingly. This indirect trust propagation allows for faster identification of malicious nodes but also introduces a potential risk of trust manipulation. The propagation mechanism follows a weighted averaging approach.

$$T_{k,y}(t) = \frac{T_{k,x}(t) + T_{x,y}(t)}{2} \quad (8)$$

Where node k updates its trust score for node y based on its trust in node x and the trust score that node x has assigned to node y.

F. Trust-Based DDoS Attack Detection

The proposed trust-based system is used to detect DDoS attacks by identifying nodes whose trust scores consistently fall below the set threshold due to anomalies in their behaviour. DDoS attacks typically involve a sudden surge of requests from compromised nodes, resulting in dropped packets, increased response times, and detected anomalies, all of which contribute to a rapid decline in the trust score. The detection algorithm works as follows:

1) Monitor trust values: Continuously monitor the trust values for all nodes in the network.

2) Detect malicious nodes: If a node's trust score falls below the threshold T_{thresh}, flag the node as suspicious.

3) Isolate suspicious nodes: Once flagged, restrict the node's ability to communicate with other nodes until further investigation is carried out or the node is cleared.

IV. Trust-Based DDoS Detection System

In this section, we delve deeper into the workings of our proposed trust-based system for detecting Distributed Denial of Service (DDoS) attacks in smart home networks. The system uses trust scores to detect anomalies in node behaviour that could indicate a malicious DDoS attack. By dynamically assessing the trustworthiness of each node, our system can identify compromised nodes that are part of a DDoS attack and take action to mitigate the attack in real time.

A. Trust Propagation and Decision Making

The trust-based DDoS detection system operates by continuously monitoring and updating trust values between nodes. Each IoT device in the network maintains a trust score for other devices it communicates with. Trust propagation ensures that trust information is shared across the network, allowing for more comprehensive decision-making.

1) Trust evaluation: Trust values are evaluated based on the behaviour of the nodes, as discussed in Section III(B). Nodes

regularly assess their neighbours based on metrics such as Packet Delivery Ratio (PDR), Response Time (RT), and Anomaly Detection (AD). A node that behaves consistently within normal parameters maintains a high trust score. Conversely, a node that shows erratic or malicious behaviour, such as failing to forward packets or exhibiting a high rate of traffic anomalies, will experience a drop in trust.

2) Trust propagation and aggregation: Trust propagation allows nodes to share their trust evaluations of other nodes, leading to a more informed decision-making process. If node x trusts node y but receives reports from other nodes indicating low trust in y, node x can adjust its trust value for y accordingly. This aggregation of trust values helps quickly isolate malicious nodes. Trust propagation is defined mathematically as follows:

$$T_{x,y}(t+1) = \frac{T_{x,y}(t) + \sum_{m \in N(x)} T_{m,y}(t)}{N(x)+1} \quad (9)$$

Where:

$T_{(x,y)}(t+1)$ is the trust value between nodes x and y at time t.

$N_{(x)}$ is the set of neighbouring nodes if x,

$T_{(m,y)}(t)$ is the trust value that node m assigns to node y.

This formula ensures that a node's trust score reflects not only its direct interactions but also the observations of other nodes in the network. This collective trust evaluation reduces the likelihood of isolated nodes manipulating their trust values to avoid detection.

B. DDoS Detection Algorithm

The detection of DDoS attacks in the trust-based system relies on identifying nodes with consistently low trust scores. These low scores indicate misbehaviour such as failing to forward packets, delaying responses, or generating abnormally high traffic. The following algorithm outlines the detection process:

1) Step 1: Initialize Trust Values: Each node x in the network initializes a trust score T(x,y)(0) for every other node y. The initial trust value is set to a neutral level, such as 0.5.

2) Step 2: Continuous Monitoring: Nodes continuously monitor the behaviour of their neighbours based on the metrics discussed in Section III(B) (Packet Delivery Ratio, Response Time, and Anomaly Detection).

3) Step 3: Trust Score Update: Each node x updates its trust score for every other node y after each interaction. The updated trust score T(x,y)(t) is calculated using the formula described in Section III(B).

4) Step 4: Threshold Comparison: At regular intervals, each node compares the trust score of its neighbours to a predefined threshold T_{thresh}. If the trust score $T_{(x,y)}(t)$ falls below T_{thresh} node y is flagged as suspicious.

If $T_{x,y}(t) < T_{thresh}$ then node j is flagged as suspicious. (10)

5) Step 5: Quarantine Suspicious Nodes: Once a node is flagged as suspicious, the system takes preventive action. The suspicious node is quarantined, meaning its communication with other nodes is limited, and it is closely monitored. This limits the node's ability to participate in DDoS attacks. The algorithm can be represented as pseudo code as follows:

Algorithm 1: Quarantine Algorithm

```
for each node x in network:
    for each neighbour y of x:
        T[x,y] = CalculateTrust(x,y)
        if T[x,y] < T_threshold:
            FlagNode(y)
            QuarantineNode(y)
             End
```

C. Detection of Specific DDoS Attack Types

The proposed trust-based system can detect various types of DDoS attacks based on the specific behaviours they induce in the network. Below are three common types of DDoS attacks and how they are detected:

1) TCP SYN Flood detection: In a TCP SYN flood attack, a malicious node sends repeated SYN requests to overwhelm the victim node's resources. This attack results in.

a) Increased response times (since the victim node is overwhelmed).

b) Decreased Packet Delivery Ratio (as the victim node struggles to handle legitimate traffic).

The trust score of a node participating in a TCP SYN flood attack will drop due to poor Response Time (RT) and Packet Delivery Ratio (PDR). The system detects this as follows:

- Response Time Monitoring: If node x observes a consistent delay in receiving responses from node y, it will reduce the trust score T_(x,y)(t) accordingly.

$$T_{x,y}(t) = T_{x,y}(t\text{-}1) - \Delta RT_{x,y}(t) \quad (11)$$

- Packet Delivery Monitoring: If node *j* is unable to deliver packets reliably, $PDR_{(x,y)}(t)$ will decrease, leading to a further reduction in trust.

$$T_{x,y}(t) = T_{x,y}(t\text{-}1) - \Delta PDR_{x,y}(t) \quad (12)$$

2) HTTP Flood detection: In an HTTP flood attack, a compromised node generates a high volume of HTTP requests to overload the victim's web services. This leads to:

- Abnormally high traffic generation.
- Anomalies detected in traffic patterns (AD).

The proposed trust-based system detects HTTP flood attacks by monitoring traffic volumes and identifying anomalies in the behaviour of nodes. Nodes that generate an unusually high number of HTTP requests will be flagged based on their Anomaly Detection (AD) score:

$$AD_{x,y}(t) = \begin{cases} 1 & \text{if no anomaly is detected,} \\ 0 & \text{if an anomaly is detected.} \end{cases} \quad (13)$$

A lower AD score leads to a drop in the overall trust value $T_{(x,y)}(t)$, eventually flagging the node as suspicious.

3) UDP Flood detection: A UDP flood attack involves sending large volumes of UDP packets to flood the victim's bandwidth. This results in: This leads to:

- High packet loss.
- Poor packet delivery ratio (PDR).

In this case, the system detects the attack by monitoring the Packet Delivery Ratio (PDR) of affected nodes. If node x observes that node y is consistently dropping packets, the trust score for node y is reduced:

$$PDR_{x,y}(t) = \frac{\text{Packets Delivered by node y}}{\text{Total Packets Sent to node y}} \quad (14)$$

A low PDR leads to a decline in trust:

$$T_{x,y}(t) = T_{x,y}(t\text{-}1) - \Delta PDR_{x,y}(t) \quad (15)$$

D. Mitigation Strategy

The detection of DDoS attacks in the trust-based system relies on identifying nodes with consistently low trust scores. These low scores indicate misbehaviour such as failing to forward packets, delaying responses, or generating abnormally high traffic. The following algorithm outlines the detection process:

1) Node quarantine: The system temporarily restricts the suspicious node's ability to communicate with other nodes in the network. This reduces the likelihood of the node participating in a DDoS attack. During quarantine, the system continues to monitor the node's behaviour.

2) Traffic filtering: Suspicious traffic from flagged nodes is filtered to prevent it from overwhelming legitimate network resources. The system prioritizes traffic from trusted nodes, ensuring that the network remains functional even during an ongoing attack.

3) Reassessment of trust: After a predefined period, the system re-evaluates the trust score of quarantined nodes. If the node's behaviour improves (e.g., it no longer generates anomalies or has improved packet delivery), the node can be re-integrated into the network. Otherwise, it remains quarantined or is permanently blacklisted.

V. Result and Analysis

To evaluate the performance of the proposed model, a simulation was carried out using OMNET++ simulator which was selected due to its platform independence and pre-defined function. To implement the trust-based detection system, we extend the IoT device modules with trust evaluation functionality. Each device calculates the trust score of its neighbours based on their behaviour (packet delivery, response time, and anomaly detection). We measured the following performance metrics:

- Malicious Attack Detection Rate: The percentage of malicious nodes correctly identified by the system.
- False Positive Rate: The percentage of benign nodes incorrectly flagged as malicious.
- Latency: The average time taken to detect and mitigate a DDoS attack.
- Network Throughput: The total amount of data successfully transmitted across the network, indicating the impact of DDoS attacks on network performance.

The complete simulation setup is illustrated in Table I.

TABLE I. Common Simulation Parameters

Simulation environment	Values
Simulator	OMNET++ v 6.0.2
Platform	Windows 11
Number of Nodes	10-50
Time Interval	100-1000s
Topology	800m X 600m
Communication Range	50m
Default Trust Value	0.5
Trust Threshold Value	Data Link
Malicious Penalty	0.2
Decay Rate	0.99
Legitimate Reward	0.1

A. Malicious Attack Detection Rate

The percentage of malicious nodes correctly identified by the trust-based DDoS detection system is evaluated against TCP, UDP and HHTP flood attacks. The simulation results are captured and analysed based on the performance metrics. Table II show is a summary of the results:

TABLE II. Detection Rate

Attack Type	Detection Rate (%)
TCP SYN Flood	98
UDP Flood	95
HTTP Flood	92

Fig. 2 illustrates the comparison of our system with existing approaches and demonstrates that a higher detection rate is obtained by the system. The distributed denial-of-service detection mechanism (DiDDeM) system showed a 92% detection rate for TCP SYN flood attacks, 91% for UDP flood attacks and 88% for HTTP flood attacks. Whilst the Adaptive threshold algorithm (ATA) has a detection rate of 93.85%, 92% and 89% respectively for all three attack types. Our trust-based detection system successfully detects most DDoS attacks, with a high detection rate across all attack types tested.

B. False Positive Rate

This is a measure of the percentage of benign nodes incorrectly flagged as malicious. Fig. 3 shows the results of the simulation of our system in comparison to other known systems including the Hybrid Deep Learning CNN-GRU model and the Adaptive threshold algorithm (ATA).

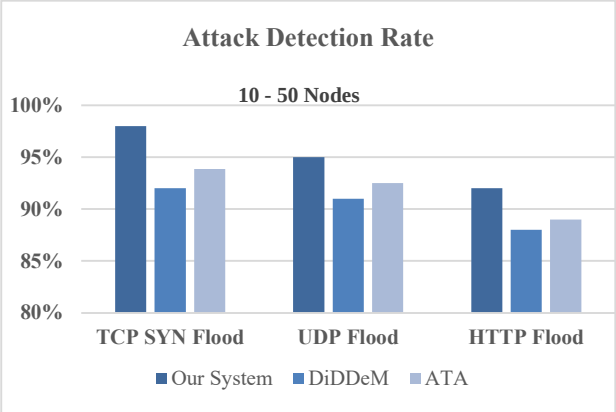

Fig. 2. Malicious attack detection rate.

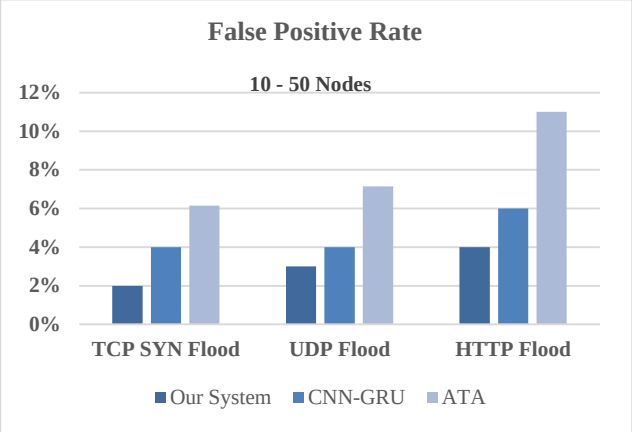

Fig. 3. False positive rate.

The system maintains a low false positive rate (Table III), ensuring that most benign nodes are not incorrectly flagged as malicious.

TABLE III. FALSE POSITIVE RATE

Attack Type	False Positive Rate (%)
TCP SYN Flood	2
UDP Flood	3
HTTP Flood	4

C. Latency

This refers to the delay introduced by the trust calculation and decision-making process. The trust-based system detects attacks with minimal latency (20–22ms), balancing trust evaluation overhead with efficient traffic forwarding and allowing for real-time mitigation. The simulation results are captured and analysed based on the performance metrics. Table IV show is a summary of the results:

TABLE IV. LATENCY

Attack Type	Detection Latency (ms)
TCP SYN Flood	20
UDP Flood	21
HTTP Flood	22

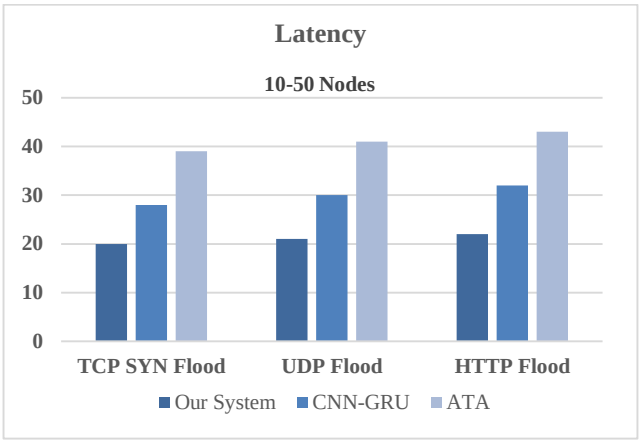

Fig. 4. Latency.

Fig. 4 illustrates the comparison of our system with other existing approaches. The Hybrid Deep Learning CNN-GRU model has the highest latency (28–32ms), due to computationally intensive traffic analysis and the Adaptive threshold algorithm (ATA) has a moderate latency (39-43ms) due to the additional analysis performed beyond threshold enforcement.

D. Network Throughput

This is a measure of the percentage of legitimate traffic successfully forwarded after isolating malicious nodes. Benign nodes that are incorrectly flagged as malicious. Table V. shows the results of the simulation of the system.

TABLE V. NETWORK THROUGHPUT

Attack Type	Throughput (Mbps) Before Attack	Throughput (Mbps) During Attack	Throughput (Mbps) After Detection
TCP SYN Flood	100	50	90
UDP Flood	100	40	85
HTTP Flood	100	45	88

The network throughput drops significantly during an attack but recovers after the trust-based system detects and mitigates the attack. The system maintained a high throughput even after detection (TCP - 95%, UDP - 85% and HTTP - 88%) by isolating only malicious nodes, ensuring minimal disruption to legitimate traffic. There were no instances of occasionally dropping legitimate traffic due to misclassification.

VI. CONCLUSION AND FUTURE WORK

Our proposed trust-based detection mechanism for Distributed Denial of Service (DDoS) attacks in SHIoT networks demonstrates significant potential to improve the security and resilience of SHIoT environments. By utilizing trust scores, the system efficiently identifies and isolates malicious nodes while ensuring minimal impact on legitimate traffic. This research highlights the critical need for adaptive, lightweight, and scalable security solutions tailored to resource-constrained IoT environments. The integration of trust-based mechanisms tailored to SHIoT environments enables the mechanism to detect and mitigate multiple types of DDoS attacks, including TCP SYN Flood, HTTP Flood, and UDP Flood. Our technique

prioritizes lightweight computation to accommodate the limited processing and energy capacities of SHIoT devices. We achieve high detection accuracy, correctly identifying malicious nodes within a short time frame while maintaining a low false positive rate. This ensures the reliability of the network and protects against unnecessary isolation of legitimate nodes. The use of trust decay, penalties for malicious behaviour, and rewards for legitimate traffic ensures that trust scores dynamically reflect the behaviour of each node. This adaptability makes our technique robust against evolving attack patterns and intermittent malicious activities.

This research addresses a critical gap in SHIoT security by providing a lightweight yet effective solution for DDoS detection. As SHIoT adoption continues to grow, securing these networks would continue to be imperative in a bid to prevent disruptions, enhance the resilience of smart home networks, and ensure the integrity, privacy, and availability of SHIoT communications. Our proposed trust-based detection technique not only lays a strong foundation for SHIoT security but also opens avenues for further innovation. The findings of this study reinforce the importance of trust-based approaches in combating cyber threats in IoT networks and paves the way for the development of more secure and reliable IoT systems, ensuring a safer and better-connected future. Future research could explore the design of a scalable, trust-based, easily adaptable cloud/edge computing infrastructure as a service solution for SHIoT networks.

ACKNOWLEDGMENT

The authors would like to acknowledge the support of the Nottingham Trent University (NTU) for a fully funded studentship. The authors also declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] T. Magara and Y. Zhou, "Internet of Things (IoT) of Smart Homes: Privacy and Security," Journal of Electrical and Computer Engineering, vol. 2024, (1), pp. 7716956, 2024.

[2] A. M. Ansari, M. Nazir and K. Mustafa, "Smart Homes App Vulnerabilities, Threats, and Solutions: A Systematic Literature Review," Journal of Network and Systems Management, vol. 32, (2), pp. 29, 2024.

[3] M. K. Wyrwicka, E. Więcek-Janka and Ł Brzeziński, "Transition to sustainable energy system for Smart Cities—Literature Review," Energies, vol. 16, (21), pp. 7224, 2023.

[4] M. Khalid, "Smart grids and renewable energy systems: Perspectives and grid integration challenges," Energy Strategy Reviews, vol. 51, pp. 101299, 2024.

[5] A. H. Mohammed and R. M. A. Hussein, "A security services for internet of thing smart health care solutions based blockchain technology," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 20, (4), pp. 772-779, 2022.

[6] A. Y. Dawod, M. F. Abdulqader and Q. M. Zainel, "Enhancing Security and Sensors Emerging Internet of Things (IoT) Technology of Homophone-Based Encryption using MANET-IoT Networks Technique," Journal of Electrical Systems, vol. 20, (6s), pp. 1345-1351, 2024.

[7] K. Murat et al, "Security Analysis of Low-Budget IoT Smart Home Appliances Embedded Software and Connectivity," Electronics, vol. 13, (12), pp. 2371, 2024.

[8] N. Solangi et al, "IoT based home automation system: Security challenges and solutions," in 2024 5th International Conference on Advancements in Computational Sciences (ICACS), 2024.

[9] I. Cvitić et al, "An overview of smart home iot trends and related cybersecurity challenges," Mobile Networks and Applications, vol. 28, (4), pp. 1334-1348, 2023.

[10] A. Aldahmani et al, "Cyber-security of embedded IoTs in smart homes: challenges, requirements, countermeasures, and trends," IEEE Open Journal of Vehicular Technology, vol. 4, pp. 281-292, 2023.

[11] A. M. Al-Ghaili et al, "A review on role of image processing techniques to enhancing security of IoT applications," IEEE Access, vol. 11, pp. 101924-101948, 2023.

[12] D. Singla et al, "Blockchain-powered healthcare: Revolutionizing security and privacy in IoT-based systems," in 2024 International Conference on Computational Intelligence and Computing Applications (ICCICA), 2024.

[13] H. Yang, Y. Guo and Y. Guo, "Blockchain-based cloud-fog collaborative smart home authentication scheme," Computer Networks, vol. 242, pp. 110240, 2024.

[14] Z. Zheng and H. Nazif, "An energy-aware technique for resource allocation in mobile internet of thing (miot) using selfish node ranking and an optimization algorithm," IETE Journal of Research, vol. 70, (4), pp. 3546-3571, 2024.

[15] A. Allen et al, "Smart homes under siege: Assessing the robustness of physical security against wireless network attacks," Comput. Secur., vol. 139, pp. 103687, 2024.

[16] M. R. Ahmed and M. O. Rahman, "An Enhanced Secure User Authentication and Authorized Scheme for Smart Home Management." International Journal of Advanced Computer Science & Applications, vol. 15, (6), 2024.

[17] P. Shukla, C. R. Krishna and N. V. Patil, "Iot traffic-based DDoS attacks detection mechanisms: A comprehensive review," The Journal of Supercomputing, vol. 80, (7), pp. 9986-10043, 2024.

[18] D. S. Gonçalves, R. S. Couto and M. G. Rubinstein, "A protection system against HTTP flood attacks using software defined networking," Journal of Network and Systems Management, vol. 31, (1), pp. 16, 2023.

[19] S. Marleau, P. Rahman and C. Lung, "DDoS flood detection and mitigation using SDN and network ingress filtering-an experiment report," in 2024 IEEE 4th International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB), 2024.

[20] O. M. Almorabea et al, "IoT Network-Based Intrusion Detection Framework: A Solution to Process Ping Floods Originating From Embedded Devices," IEEE Access, vol. 11, pp. 119118-119145, 2023.

[21] J. Lee et al, "Rescuing QUIC flows from countermeasures against UDP flooding attacks," in Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing, 2024.

[22] S. Evmorfos et al, "Neural network architectures for the detection of SYN flood attacks in IoT systems," in Proceedings of the 13th ACM International Conference on PErvasive Technologies Related to Assistive Environments, 2020.

[23] R. Bensaid et al, "Toward a Real - Time TCP SYN Flood DDoS Mitigation Using Adaptive Neuro - Fuzzy Classifier and SDN Assistance in Fog Computing," Security and Communication Networks, vol. 2024, (1), pp. 6651584, 2024.

[24] M. Azrour et al, "Internet of things security: challenges and key issues," Security and Communication Networks, vol. 2021, (1), pp. 5533843, 2021.

[25] S. Karnani, N. Agrawal and R. Kumar, "A comprehensive survey on low-rate and high-rate DDoS defense approaches in SDN: taxonomy, research challenges, and opportunities," Multimedia Tools Appl, vol. 83, (12), pp. 35253-35306, 2024.

[26] M. Patel et al, "DDoS Attack Detection Model using Machine Learning Algorithm in Next Generation Firewall," Procedia Computer Science, vol. 233, pp. 175-183, 2024.

[27] R. N. Bashir et al, "Smart reference evapotranspiration using Internet of Things and hybrid ensemble machine learning approach," Internet of Things, vol. 24, pp. 100962, 2023.

[28] H. I. Mhaibes, M. H. Abood and A. K. Farhan, "Simple Lightweight Cryptographic Algorithm to Secure Imbedded IoT Devices." International Journal of Interactive Mobile Technologies, vol. 16, (20), 2022.

[29] O. Okporokpo et al, "Trust-based Approaches Towards Enhancing IoT Security: A Systematic Literature Review," arXiv Preprint arXiv:2311.11705, 2023.

[30] S. M. Muzammal, R. K. Murugesan and N. Z. Jhanjhi, "A comprehensive review on secure routing in internet of things: Mitigation methods and trust-based approaches," IEEE Internet of Things Journal, vol. 8, (6), pp. 4186-4210, 2020.

[31] H. Tyagi, R. Kumar and S. K. Pandey, "A detailed study on trust management techniques for security and privacy in IoT: Challenges, trends, and research directions," High-Confidence Computing, pp. 100127, 2023.

[32] M. Nikravan and M. Haghi Kashani, "A review on trust management in fog/edge computing: Techniques, trends, and challenges," Journal of Network and Computer Applications, vol. 204, pp. 103402, 2022. Available: https://www.sciencedirect.com/science/article/pii/S1084804522000613. DOI: 10.1016/j.jnca.2022.103402.

[33] A. Shuhaiber and I. Mashal, "A multi-layered trust model in the internet of things smart home ecosystem," in 2024 11th International Conference on Wireless Networks and Mobile Communications (WINCOM), 2024.

[34] K. Ahmadi, R. Javidan and H. Park, "A Trust Based Anomaly Detection Scheme Using a Hybrid Deep Learning Model for IoT Routing Attacks Mitigation." IET Information Security (Wiley-Blackwell), vol. 2024, 2024.

[35] S. Singh, V. Anand and S. Yadav, "Trust-based clustering and routing in WSNs using DST-WOA," Peer-to-Peer Networking and Applications, pp. 1-13, 2024.

[36] A. Padma and M. Ramaiah, "GLSBIoT: GWO-based enhancement for lightweight scalable blockchain for IoT with trust based consensus," Future Generation Comput. Syst., vol. 159, pp. 64-76, 2024.

[37] F. Azzedin, "Mitigating denial of service attacks in RPL-based IoT environments: trust-based approach," IEEE Access, vol. 11, pp. 129077-129089, 2023.