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

Ingénierie des Systèmes d'Information
Vol. 30, No. 2, February, 2025, pp. 419-426
Journal homepage: http://iieta.org/journals/isi

Securing eNode-B from DDoS Attacks Using Isolation Bandwidth Technique

Saif Ibrahim Mezaal[1], Ahmad Hani El Fawal[2,3*]

[1] Information Technology Department, Faculty of Languages, University of Baghdad, Baghdad 10011, Iraq
[2] Lab-STICC, UMR 6285 - CNRS, ENSTA Bretagne, Brest 29806, France
[3] CS Department, Modern University for Business & Science, Damour 5660, Lebanon

Corresponding Author Email: elfawal@ieee.org

https://doi.org/10.18280/isi.300213

Received: 20 October 2024
Revised: 5 January 2025
Accepted: 14 February 2025
Available online: 27 February 2025

Keywords:
DDoS, IoT, LTE-A, LTE-M, M2M, H2H, NB-IoT

ABSTRACT

In order to defend Long-Term Evolution-Advanced (LTE-A) networks against Distributed Denial of Service (DDoS) assaults that target Machine-to-Machine (M2M) traffic, we present a novel technique in this research termed the Isolation Bandwidth Technique (IBT). Maintaining a good Quality of Service (QoS) for Human-to-Human (H2H) traffic while guaranteeing continuous availability of M2M communications is the primary objective of IBT. The rapid growth of Internet of Things (IoT) devices, projected to exceed tens of billions in the near future, introduces significant security challenges. Many IoT devices lack robust security mechanisms, making them vulnerable to exploitation in DDoS attacks, where botnets overwhelm networks with malicious traffic. LTE-A networks, designed to support massive IoT connectivity, are particularly susceptible to performance degradation, including increased latency and reduced throughput, under such attack scenarios. To address these challenges, IBT mitigates the risk of network overload during DDoS assaults by allocating a portion of the bandwidth to M2M traffic while reserving the remaining bandwidth for H2H traffic. Narrowband Internet of Things (NB-IoT) further ensures efficient M2M communication by designating specific bandwidth for suspicious traffic. This approach not only prevents malicious M2M data from disrupting the network but also sustains QoS for legitimate H2H and M2M communications.

1. INTRODUCTION

The Internet of Things (IoT) has significantly transformed industries like smart cities and agriculture by facilitating data-driven processes, increasing efficiency, and enhancing creativity through device connectivity [1]. The rapid development of IoT has led to its integration into more fields, making it a fundamental component of modern infrastructure [2, 3]. The number of IoT connections is projected to grow significantly, with estimates suggesting that it will reach 27 billion by 2025, and a staggering 125 billion devices used globally by 2030 [4]. Long-Term Evolution-Advanced (LTE-A) networks were initially designed for H2H communication, offering services like video streaming, Voice over Internet Protocol (VoIP), and File Transfer Protocol (FTP). The growing use of IoT devices and M2M traffic presents challenges in maintaining sustainable Quality of Service for both Machine-to-Machine (M2M) and Human-to-Human (H2H) traffic [5, 6].

New M2M technologies, such as Narrowband Internet of Things (NB-IoT), are expected to cater to IoT needs in future mobile networks with limited bandwidth [7]. Despite their potential benefits, these networks are vulnerable to network saturations due to DDoS attacks, which use botnets to flood networks with massive fake requests [8]. Attacks on NB-IoT limited bandwidth can easily overwhelm it.

The growing use of IoT devices raises concerns about network resource security, particularly in NB-IoT networks, where DDoS attacks pose a significant threat [9].

NB-IoT networks face security challenges like electronic intrusions, digital espionage, eavesdropping, and data manipulation. Access control, identity management, and defending against DDoS attacks and intrusions are also challenges. Botnets, compromised networks, can execute DDoS attacks without users' knowledge [10, 11].

Researchers are exploring Blockchain-based methods to counter DDoS attacks on IoT devices, including distributed engineering, traffic control, and Ethereum-based solutions, with future research focusing on their working standards and weaknesses [12].

The study [13] used the Canadian Institute for Cybersecurity Intrusion Detection System (CICIDS) 2017 dataset to study DDoS attacks in a cloud context. They developed a Machine Learning model predicting DDoS and bot attacks, achieving 97.86% accuracy.

The study [6] introduced the "LTE-M Adaptive eNodeB" scheme to efficiently manage network resources and improve M2M traffic in an IoT environment.

3GPP introduced NB-IoT to manage congestion in LTE-A networks caused by H2H and M2M traffic coexistence. NB-IoT limits M2M bandwidth, reducing congestion and ensuring smooth H2H traffic. An adaptive eNodeB (A-eNB) addresses

network overload, and the study [8] proposed using Continuous Time Markov Chain (CTMC) for coexistence during disaster scenarios.

The study [11] tackled DDoS attacks in LTE-A networks with an algorithmic load balancing defense, efficiently distributing voice and data resources. Simulations showed enhanced traffic efficiency and resource optimization without extra infrastructure. Future studies will investigate the algorithm's real-world performance in LTE networks.

LTE/LTE-A research utilizes tools like LTE-Sim and NS-3 to simulate downlink scheduler algorithms, crucial for radio resource management. Zinno et al. [14] can choose platforms based on study focus and traffic conditions. NS-3 offers tutorials and source codes, while LTE-Sim has strong community support. Both are compatible with open-source Linux for easy installation.

Do et al. [15] optimized NB-IoT and LTE paging coexistence by designing a method to calculate Paging Occasions and creating a Paging store to handle 200-300 messages per second, improving efficiency.

Hara et al. [16] developed a semi-supervised learning method using an Automatic Adversarial Encoder (AAE) to identify failure causes in LTE eNodeB base stations. The method, utilizing unlabeled data, achieved 94% accuracy with eNodeB log data from a service provider, outperforming traditional techniques in F1 score. With a labeled dataset of 220-270, it obtained 94% accuracy; for each category with more than 50 labeled data points, it scored above 91% accuracy.

Previous researchers proposed various DDoS mitigation techniques, but none isolated the malicious traffic in a separate channel to avoid the attack's impact on regular traffic. In this context, we propose using an isolation channel as a solution for DDoS attacks.

This paper aims to explore the challenges and effects of DDoS attacks on M2M and H2H traffic in LTE-A/NB-IoT networks, contributing the following:

(1) Introducing a novel IBT that allocates dedicated bandwidth for malicious M2M traffic to protect networks.
(2) Analyzing the impact of DDoS attacks on both H2H and M2M traffic.
(3) Providing empirical evidence and simulation-based validation demonstrating the effectiveness of IBT in mitigating DDoS attacks on M2M traffic.

2. LONG-TERM EVLUTION ADVANCED (LTE-A)

LTE-A networks are susceptible to DDoS attacks due to their architectural characteristics and resource management mechanisms, which are optimized for high-speed data transmission and massive connectivity. These vulnerabilities include limited control plane resources, such as signaling channels, which can be overwhelmed during signaling storms or volumetric attacks. Additionally, the dynamic allocation of radio resources and shared spectrum for both M2M and H2H traffic makes LTE-A networks more prone to resource exhaustion under malicious traffic loads. Such attacks can exhaust network resources, disrupt service quality, and compromise critical communication services [17].

To protect LTE-A networks, effective threat mitigation strategies are crucial. These include detecting and mitigating malicious traffic, enforcing access control policies, and employing traffic monitoring and anomaly detection algorithms. Proactive measures like this help maintain network performance and ensure availability, even during attack scenarios. networks are susceptible to DDoS attacks, which can exhaust resources and disrupt service quality. To protect them, effective threat mitigation strategies, including detecting and mitigating malicious traffic, enforcing access control policies, and using traffic monitoring and anomaly detection algorithms, are crucial. These proactive measures maintain network performance and availability.

3. MAXIMUM DATA RATES

We propose analyzing time-frequency resources and their correlation with data rates for M2M and H2H traffic to assess LTE-A and NB-IoT bandwidth capabilities and limitations. In LTE-A, a 10 ms radio frame is divided into ten 1 ms subframes, each split into two 0.5 ms slots, with seven symbols per slot. Time-frequency resources are organized as follows:

(1) Resource Element (RE): 15 KHz sub-carrier for one symbol.
(2) Resource Block (RB): 180 KHz, 12 sub-carriers for one slot.
(3) Physical Resource Block (PRB): 180 KHz, 12 sub-carriers for one subframe.

Consequently, a PRB has $7\times12\times2 = 168$ REs, whereas an RB has $7\times12 = 84$ REs. Furthermore, the smallest unit that can be allotted for a User Equipment (UE) to send or receive data is represented by a PRB. Studying the maximum data rates in standard LTE-A and NB-IoT technologies is critical, especially when one considers a disaster scenario when over 52,000 UEs are projected to attempt to communicate their payloads concurrently.

NB-IoT technology with its limited bandwidth (180 KHz) and low data-rate (150 Kbps) must meet all IoT requirements with more than 52000 M2M devices per cell. In this context, network saturation cannot be avoided with the threat of DDoS attacks that use botnets to overload the network with massive malicious requests.

(1) During normal cycle traffic, LTE-A networks employ 99 PRBs to fulfill H2H requests.
(2) While NB-IoT networks use 1 PRB only to serve M2M requests.

By doing our calculations, NB-IoT networks can provide a maximum data rate of (150 Kbps). Now, if we know that a Mirai attack speed is about 600 Gbps, we conclude that NB-IoT network will be overloaded when facing such attacks.

4. THE IMPACT OF DDoS ATTACKS ON LTE-A and NB-IoT Networks

The study explores the impact of DDoS attacks on LTE-A and NB-IoT networks, focusing on their impact on resource allocation and bandwidth utilization for H2H and M2M traffic.

4.1 Normal cycle analysis

NB-IoT efficiently handles M2M traffic with minimal bandwidth allocation of 1 PRB, providing reliable, energy-efficient connectivity for IoT devices. In contrast, LTE-A allocates 99 PRBs for H2H traffic, supporting scalable, high-quality connections and enhancing overall network performance and user experience, as shown in the Figure 1.

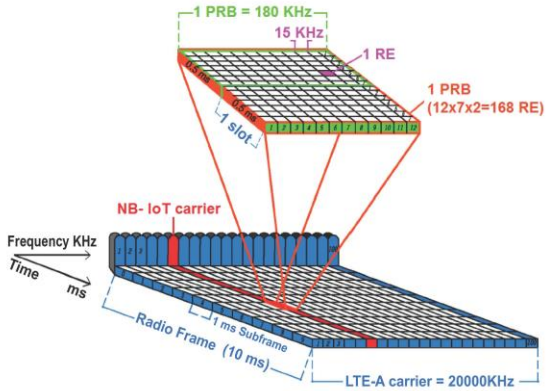

Figure 1. Normal cycle (before attack) [8]

(1) M2M Normal Traffic: In a normal M2M traffic cycle, NB-IoT technology efficiently uses 1 PRB bandwidth, meeting the specific needs of low data rates and low-power devices. This ensures reliable, energy-efficient connectivity for a broad range of IoT devices, ensuring optimal resource allocation.
(2) H2H Normal Traffic: LTE-A technology efficiently manages H2H traffic by allocating 99 PRBs, showcasing its scalability and capacity, ensuring reliable, superior connections for end users, improving user experience and network speed.

4.2 Attack cycle analysis

DDoS attacks significantly disrupt LTE-A/NB-IoT networks, causing network saturation and disrupting traffic cycles.

(1) M2M Traffic during DDoS Attacks: NB-IoT technology can handle M2M traffic with a 150 Kbps data rate, but DDoS attacks like Mirai can overload bandwidth, disrupting M2M applications. Addressing vulnerability and ensuring capacity to handle high loads is crucial for IoT applications.
(2) H2H Traffic during Attack Cycles: LTE-A technology manages H2H traffic with 99 PRBs, but DDoS attacks affect networks, necessitating effective mitigation strategies for bandwidths like 1.4 MHz, 3 MHz, and 5 MHz, ensuring QoS.

4.3 IBT for mitigating DDoS attacks

Isolation techniques are crucial for securing LTE-A networks and protecting individual eNodeBs, preventing malicious traffic transmission to other network components by containing attack effects, as illustrated in Figure 2.

The IBT allocates bandwidth for M2M malicious traffic, preventing DDoS attacks from dominating the entire PRB allocation. This strategy maintains efficient communication for M2M applications while preserving resources for legitimate traffic and minimizing LTE-A impact.

4.4 Post-attack cycle

LTE-A and NB-IoT effectively manage H2H and M2M traffic after DDoS attacks, maintaining reliable connectivity and seamless communication among IoT devices with minimal allocation of PRBs.

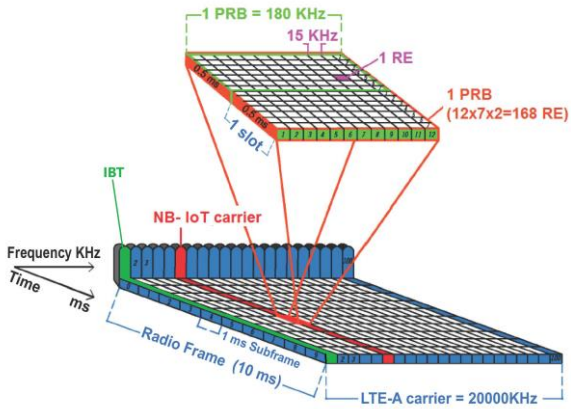

Figure 2. IBT solution

(1) M2M Traffic: NB-IoT bandwidth efficiently manages low data rate and low-power M2M communication, even after DDoS attacks, by allocating 1 PRB, demonstrating its effectiveness in seamless communication among IoT devices. However, M2M communications face specific challenges during DDoS attacks. The frequent and high-volume malicious traffic directed at the control and data planes can disrupt synchronization, leading to packet loss, delays, and the inability of M2M devices to maintain stable connections. This is particularly critical for time-sensitive IoT applications, such as industrial automation and healthcare monitoring, which rely on consistent and reliable data transmission. IBT mitigates these effects by isolating and managing suspicious traffic, ensuring continuous communication for legitimate M2M devices.
(2) H2H Traffic: After a DDoS attack, the IBT deactivates, and LTE-A bandwidth returns to normal, serving H2H traffic with 99 PRBs. This restores LTE-A's capacity for reliable H2H communication. Securing LTE-A networks against DDoS attacks with IBT is crucial for maintaining network integrity and performance. Implementing threat mitigation, isolation mechanisms, and network redundancy is essential for protecting LTE-A/NB-IoT networks and ensuring continuous service operation, as shown in the Figure 3.

The scheme depicted Network state normally, during attack and post attack

(1) Normal cycle: our LTE-A technology handles H2H traffic with minimal bandwidth allocation (100 PRBs) We take (1 PRB) to NB-IoT and it becomes (99 PRBs). Our NB-IoT delivers M2M traffic with minimal bandwidth allocation (1 PRB).

LTE-A handles H2H traffic with minimal bandwidth allocation (99 PRBs).

Our NB-IoT technology (1PRB), natively handles M2M traffic with a minimum bandwidth allocation (IPRB).

(2) DDoS Attack cycle: LTE-A handles H2H traffic with allocation (98 PRBs). Malicious M2M traffic is directed to them.

We stream NB-IoT traffic to M2M with minimum bandwidth allocation (1 PRB).

(3) If the DDoS attack continues, we will continue the attack.
(4) Post attack Cycle: when the attack ends, we will return to the normal cycle and NB-IoT will return to (1 PRB) for M2M traffic * and LTE-A with H2H traffic with an allocation of (99 PRBs).

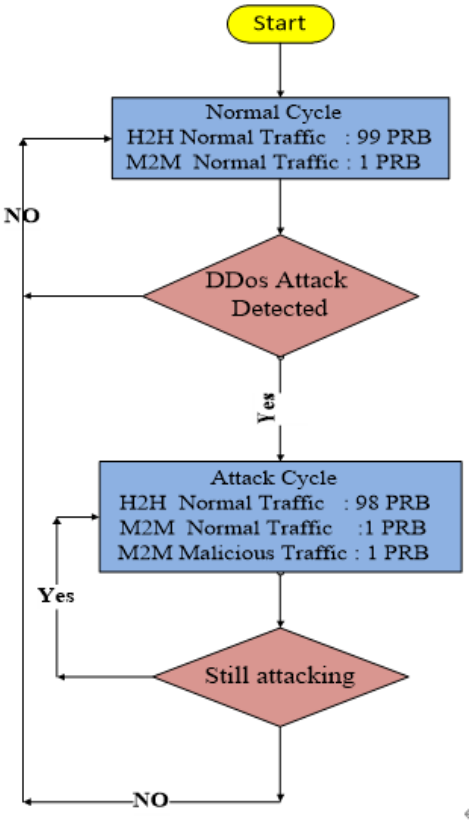

Figure 3. Flowchart of the IBT solution

4.5 Comparison with existing DDoS defense mechanisms

The IBT offers unique advantages compared to traditional DDoS defense mechanisms such as traffic cleansing and blacklisting [18]. Table 1 provides a comparison of these methods in terms of detection accuracy, response speed, resource efficiency, and adaptability to IoT environments.

4.6 Advantages of IBT over existing methods

(1) Proactive Isolation: Unlike traffic cleansing, which reacts after an attack is detected, IBT preemptively allocates bandwidth for malicious traffic, preventing it from overwhelming the network.
(2) Reduced Computational Overhead: Traffic cleansing and blacklisting require extensive traffic analysis or frequent updates, which can be resource-intensive. IBT simplifies this by isolating and managing M2M traffic based on predefined bandwidth allocation.
(3) IoT-Specific Design: Traffic cleansing and blacklisting often fail to account for the unique characteristics of IoT networks, such as low-power, low-bandwidth communication. IBT is specifically designed for IoT, ensuring seamless operation for both H2H and M2M traffic during and after an attack.
(4) Faster Response: The IBT scheme's pre-allocation of bandwidth ensures immediate containment of malicious traffic, unlike traditional methods that may take time to detect and act.

4.7 Limitations of existing methods addressed by IBT

(1) Traffic Cleansing: While effective in large-scale traditional networks, it introduces latency and is computationally expensive, making it less suitable for IoT. IBT eliminates the need for continuous traffic filtering by directly isolating suspicious traffic.
(2) Blacklisting: This method relies on maintaining and updating extensive lists of malicious IPs or sources, which can be ineffective against dynamic and distributed IoT botnets. IBT bypasses this limitation by focusing on bandwidth allocation rather than source identification.

Table 1. Comparison of IBT with existing DDoS defense mechanisms

Aspect	Traffic Cleansing	Blacklisting	IBT Scheme
Detection Accuracy	Medium: Requires advanced algorithms to differentiate malicious and legitimate traffic.	Medium: Depends on accurate and updated blacklists.	High: IBT dynamically isolates suspicious traffic, reducing false positives.
Response Speed	Moderate: Cleansing involves filtering large volumes of traffic, which may introduce delays.	High: Blocking traffic from blacklisted sources is immediate.	High: IBT pre-allocates bandwidth for malicious M2M traffic, ensuring rapid isolation.
Resource Efficiency	Low: Significant computational resources are needed for real-time traffic analysis.	Medium: Blacklisting uses fewer resources but can still be resource-intensive in large-scale attacks.	High: IBT optimizes bandwidth usage by limiting attack effects without analysing all traffic.
Adaptability to IoT	Low: Traffic cleansing often struggles with IoT-specific low-power, low-data-rate traffic.	Medium: Blacklists may not adapt well to dynamic IoT environments with rapidly changing IPs.	High: IBT is tailored for IoT environments by allocating bandwidth based on IoT traffic patterns.

5. CASE STUDY

This section analyzes real-life cyber-attacks on M2M devices using case studies and 3GPP technical reports. It highlights the integration of LTE-A and NB-IoT technology to manage M2M requests and ensure smooth operations. The study is structured into groups, following 3GPP GERAN TR's parameter sets, and assumes three groups attacking an LTE network simultaneously in a DDoS attack scenario.

5.1 Rationale for parameter selection

The simulation parameters for device numbers, payload sizes, and transmission rates were carefully chosen based on typical M2M traffic patterns documented in real-world case studies and 3GPP technical reports.
(1) Device Count: The number of devices in each group reflects common IoT deployment scenarios, such as small-scale environments with 150 devices (Group 1), medium-sized deployments with 200 devices (Group 2), and large-scale setups with 900 devices (Group 3). These groupings capture a range of potential device densities.

(2) Payload Size: Payload sizes (50-200 Bytes) align with common sensor data characteristics, such as readings from accelerometers and gyroscopes, which generate compact messages optimized for low-power, low-bandwidth transmission.
(3) Transmission Rates: The transmission rates (ranging from 1 message per hour to 100 messages per day) mimic the behavior of periodic IoT reporting, where sensors transmit data based on event-driven or scheduled intervals. This ensures that the parameters realistically simulate typical M2M traffic under normal conditions.

As an example, During Normal Cycle: Group Data Transmission Analysis details:

Group 1:

- Devices: 150
- Payload Size: 200 Bytes
- Transmission Rate: 1 message per hour

Daily Data Calculation:

200 Bytes × 24 messages = 4800 Bytes

Data Rate Calculation:

(4800 Bytes / 86400 Sec) × 8 bits × 150 devices = 66.666 bps

Data Rate in kbps= 66.666 / 1024 = 0.0651 kbps.

Group 2:

- Devices: 200 Accelerometer Sensors
- Transmission Rate: 8 messages per day per sensor
- Payload Size: 100 Bytes per message

Daily Data Calculation:

100 Bytes × 8 messages = 800 Bytes

Data Rate = (800 Bytes / 86400 Sec) × 8 bits × 200 devices =14.814 bps

Data Rate in kbps = 14.814 / 1024 = 0.0144 kbps.

Group 3:

- Devices: 900 Gyroscope Sensors
- Transmission Rate: 100 messages per day per sensor
- Payload Size: 50 Bytes per message

Daily Data Calculation:

50 Bytes × 100 messages = 5000 Bytes

Data Rate Calculation:

(5000 Bytes / 86400 Sec) × 8 bits × 900 devices = 416.67 bps

Data Rate in kbps = 416.67 / 1024 = 0.407 kbps.

Total Data Rate = 0.0651 + 0.0144 + 0.407 = 0.487 kbps.

By comparing the total data rate of 0.487 kbps with the maximum NB-IoT data rate of 150 kbps, we conclude that NB-IoT technology can operate smoothly during a normal cycle with no congestion problems.

5.2 During attack

In a DDoS attack scenario on M2M devices, the attacker transforms devices into "zombies" to send synchronized payloads. Three attacks are calculated:

(1) Attack1:

Data rate=(200 Bytes × 8 bits × 150 devices)/1024=234 kbps

(2) Attack2:

Data rate=(100 Bytes × 8 bits × 200 devices)/1024=156 kbps

(3) Attack3:

Data rate=(50 Bytes × 8 bits × 900 devices)/1024=351 kbps

NB-IoT technology is expected to face significant degradation and congestion issues during DDoS attacks, as evidenced by comparisons of attack storms (234 kbps, 156 kbps, 351 kbps) and maximum NB-IoT data rate (150 kbps).

5.3 IBT solution

The NB-IoT network has seen significant improvements following the implementation of IBT, resulting in a robust 300 kbps data rate. This capacity is crucial in handling DDoS attacks, as recorded data rates during attacks ranged from 234 kbps to 351 kbps. This solution effectively mitigated the impact of the first and second attacks.

6. SIMULATION

We use the open-source SimuLTE Modeler 0.9.1 within an OMNeT++ 4.6 and INET 2.3.0 environment, hosted on a cluster server. The simulation lasts sixty seconds, with a maximum distance of 300 meters between the eNodeB and User Equipment (UE), moving at 120 km/h. Three distinct scenarios are simulated.

6.1 Regular cycle scenario

A simulation of H2H traffic users, including 5 VoIP download and 5 video download users connected to LTE-A, and 20 M2M connections using 1 PRB from the NB-IoT channel, showed that VoIP traffic received the highest receiving rate at 95%, requiring high QoS. Video traffic received 73%, indicating significant network resource usage for video data transmission. M2M traffic received 61%, indicating efficient network design for M2M communication, as shown in Figure 4.

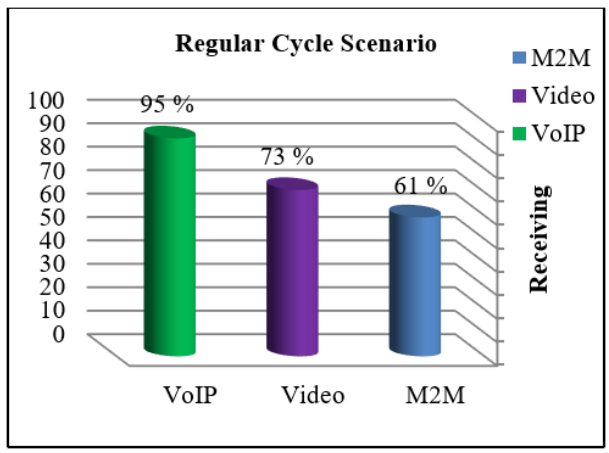

Figure 4. Regular scenario results

6.2 DDoS assault scenario

A simulated scenario of 5 VoIP downloads and video download users connected to LTE-A, 20 M2M connections, and 10 M2M Zombie links shows a significant loss in network performance during an attack, resulting in a significant decline in service quality. As shown in Figure 5.

VoIP traffic, which represents continuous voice calls, generates moderate data with a Receiving Rate (RR) of 39%. Despite its stability, it is vulnerable to attack impacts. Video traffic, representing streaming, shows a significant rise in packet count but a lower RR of 23% during the attack, greatly disrupting streaming performance.

M2M traffic, with low volumes and small packet sizes, experiences reduced performance due to network congestion. Zombie traffic, with a higher data rate, overwhelms network bandwidth with a 31% RR.

The attack significantly impacted data, with VoIP traffic experiencing reduced quality and video traffic experiencing significant data volume, highlighting the network's constraints and limitations during the attack.

M2M traffic's vulnerability is evident in quantity and packet size, while "Zombie" traffic's large data sizes and limited packet counts raise questions about network effects and role.

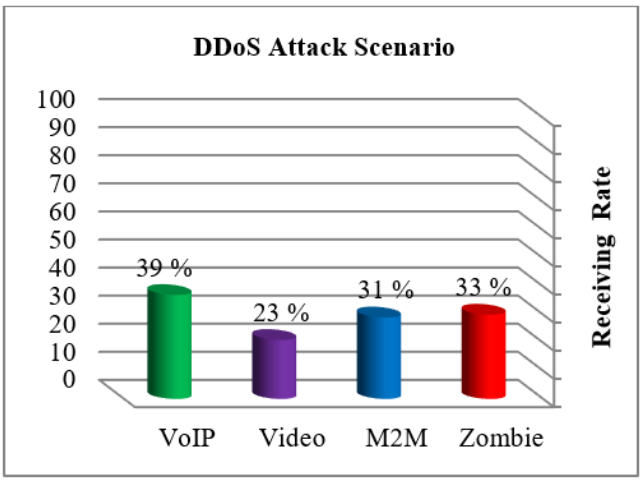

Figure 5. DDoS assault scenario results

6.3 IBT solution scenario

The simulated scenario includes 5 VoIP DL users, 5 Video-DL users on LTE-A (99 PRBs), 20 M2M devices on 1 PRB (NB-IoT channel), and 10 M2M Zombie links isolated in an IBT channel (1 PRB). The 60-second simulation shows VoIP has the highest RR of 90%, indicating significant resource allocation to VoIP traffic (Figure 6).

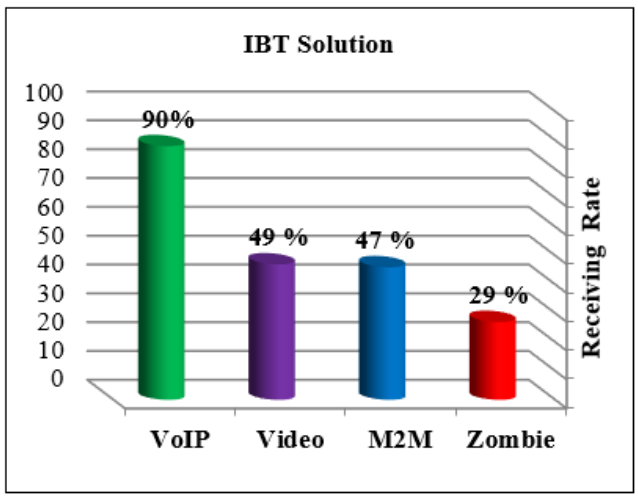

Figure 6. IBT solution scenario results

The network prioritizes VoIP communication due to its low latency and high-quality service, while video traffic has a moderately high Receiving Rate (49%), indicating high bandwidth demand. M2M traffic has a 47% RR, indicating significant network load. Zombie traffic has a 29% RR, indicating effective resource limitations due to successful isolation through IBT solution, highlighting the importance of M2M traffic in overall network load.

7. RESULT COMPARISON

7.1 Comparison of regular and attack impact

Below is the equation that describes the Impact Rate (IR) of a DDoS attack over normal traffic:

$$\text{IR} = \left(\frac{\text{RR in Regular} - \text{RR in DDoS attack}}{\text{RR in Regular}}\right) \times 100 \qquad (1)$$

This equation calculates the impact rate as a percentage, showing the drop-in success rates during an attack compared to normal conditions:

(1) VoIP Traffic: Success rate drops from 95% to 39%, with an impact rate of 58%.
(2) Video Traffic: Success rate falls from 73% to 23%, with an impact rate of 68%.
(3) M2M Traffic: Success rate decreases from 61% to 31%, with an impact rate of 49%.

These results highlight a significant negative impact on VoIP, video, and M2M services during the attack, with a sharp decline in success rates across all traffic types Figure 7.

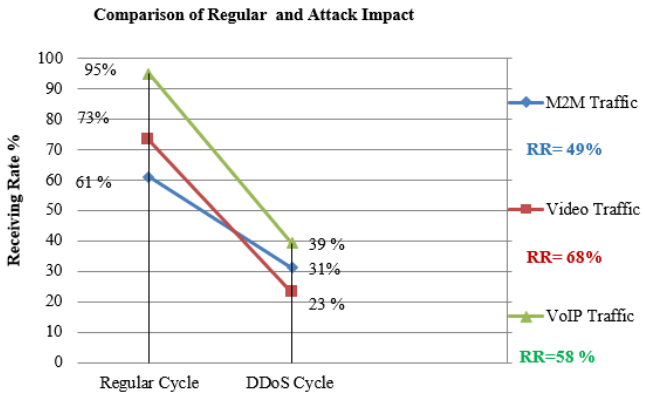

Figure 7. Comparison of regular and attack impact

7.2 Comparison of attack results and ibt solution performance

To calculate the improvement between "Attack Results" and "IBT Solution Results," you can use the following formula:

$$\text{Improvement} = \left(\frac{\text{RR in IBT} - \text{RR in DDoS attack}}{\text{RR in DDoS attack}}\right) \text{x}100 \qquad (2)$$

Improvement in VoIP Traffic:
Improvement (VoIP) = (90-39/39) ×100≈130%
Improvement in Video Traffic:
Improvement (Video) = (47-23/23) ×100≈104%
Improvement in M2M Traffic:
Improvement (M2M) = (46-31/31) ×100≈48%

These "Improvement" values indicate the percentage change in "Results IBT" compared to "Results Attack" for each traffic type, as illustrated in Figure 8.

To provide a quantitative analysis of the improvement achieved by the IBT scheme, we calculated the improvement rate for each traffic type. The improvement rate represents the percentage increase in performance when comparing attack scenarios with and without the IBT scheme.

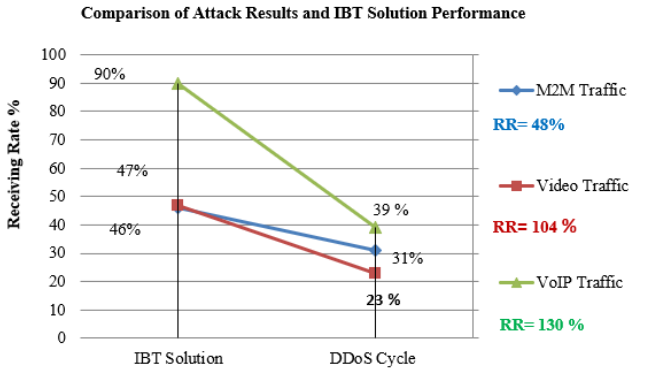

Figure 8. Comparison of attack results and IBT solution performance

$$\text{Average Improvement Rate} = \left(\frac{\text{Sum of Improvement Rates}}{\text{Number of Traffic Types}}\right) \quad (3)$$

Maximum Improvement Rate:
The highest improvement rate among all traffic types.

$$\text{Average Improvement Rate} = \left(\frac{130 + 104 + 48}{3}\right) = 94\% \quad (4)$$

Maximum Improvement Rate: 130%

For VoIP traffic, the improvement rate was 130%, while video traffic showed an improvement rate of 104%, and M2M traffic achieved a rate of 48%. On average, the IBT scheme improved network performance by 94% across all traffic types, with the maximum improvement observed in VoIP traffic at 130%. These results highlight the significant effectiveness of the IBT scheme in mitigating the impact of DDoS attacks on various traffic types.

8. CONCLUSIONS

The implementation of the IBT solution has successfully improved NB-IoT network performance during DDoS attacks. One of the most significant improvements is the increase in the network's data rate from 150 Kbps to a robust 300 Kbps, which has played a crucial role in mitigating the impact of these attacks. During such attacks, IoT devices are exploited as "zombies" to launch continuous, simultaneous assaults. Our research shows that the traditional NB-IoT network, operating at 150 Kbps, struggles to withstand these attacks. The impact rate, compared to normal conditions, is 58% for VoIP traffic, 68% for video traffic, and 49% for M2M traffic.

The increase in network bandwidth capacity, from 1 PRB to 2 PRBs, has been pivotal in managing DDoS attacks that use IoT devices as "zombies" for coordinated assaults, further highlighting the remarkable efficiency of the IBT solution in combating these threats. After implementing the IBT solution, the improvements (compared to attack results) for various types of traffic are as follows: 130% for VoIP traffic, 104% for video traffic, and 48% for M2M traffic.

Our work successfully addresses the data rate challenges posed by both initial and subsequent DDoS attacks through the intelligent application of the IBT solution. This solution represents a significant advancement in enhancing IoT security and safeguarding M2M communications within LTE-A networks.

REFERENCES

[1] Jalasri, M., Manikandan, S., Nicholas, A.D., Gobimohan, S., Rao, N.S. (2024). Hybrid optimized data aggregation for fog computing devices in internet of things. Baghdad Science Journal, 21(5S): 1811-1826. https://doi.org/10.21123/bsj.2024.10551

[2] Shah, Z., Ullah, I., Li, H., Levula, A., Khurshid, K. (2022). Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey. Sensors, 22(3): 1094. https://doi.org/10.3390/s22031094

[3] Mouha, R.A. (2021). Internet of Things (IoT). Journal of Data Analysis and Information Processing, 9(2): 77-101. https://doi.org/10.4236/jdaip.2021.92006

[4] El Fawal, A.H., Mansour, A., Ammad Uddin, M., Nasser, A. (2024). Securing IoT networks from DDoS attacks using a temporary dynamic IP strategy. Sensors, 24(13): 4287. https://doi.org/10.3390/s24134287

[5] Singh, U., Dua, A., Tanwar, S., Kumar, N., Alazab, M. (2021). A survey on LTE/LTE-A radio resource allocation techniques for machine-to-machine communication for B5G networks. IEEE Access, 9: 107976-107997. https://doi.org/10.1109/ACCESS.2021.3100541

[6] El Fawal, A.H., Mansour, A., Najem, M., Le Roy, F., Le Jeune, D. (2017). LTE-M adaptive eNodeB for emergency scenarios. In 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South), pp. 536-541. https://doi.org/10.1109/ICTC.2017.8191035

[7] Lin, Y.B., Tseng, H.C., Lin, Y.W., Chen, L.J. (2018). NB-IoTtalk: A service platform for fast development of NB-IoT applications. IEEE Internet of Things Journal, 6(1): 928-939. https://doi.org/10.1109/JIOT.2018.2865583

[8] El Fawal, A.H., Mansour, A., Najem, M., Le Roy, F., Le Jeune, D. (2018). CTMC modeling for M2M/H2H coexistence in a NB-IoT adaptive eNodeB. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, pp. 1-8. https://doi.org/10.1109/Cybermatics_2018.2018.00035

[9] Sambangi, S., Gondi, L. (2020). A machine learning approach for DDoS (distributed denial of service) attack detection using multiple linear regression. Proceedings, 63(1): 51. https://doi.org/10.3390/proceedings2020063051

[10] Doshi, K., Yilmaz, Y., Uludag, S. (2021). Timely detection and mitigation of stealthy DDoS attacks via IoT networks. IEEE Transactions on Dependable and Secure Computing, 18(5): 2164-2176. https://doi.org/10.1109/TDSC.2021.3049942

[11] Jia, Y., Zhong, F., Alrawais, A., Gong, B., Cheng, X. (2020). Flowguard: An intelligent edge defense mechanism against IoT DDoS attacks. IEEE Internet of Things Journal, 7(10): 9552-9562. https://doi.org/10.1109/JIOT.2020.2993782

[12] Shah, Z., Ullah, I., Li, H., Levula, A., Khurshid, K.

(2022). Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey. Sensors, 22(3): 1094. https://doi.org/10.3390/s22031094

[13] Staal, T.J. (2022). The impact of the Internet of Things on the demand of cloud resources. Bachelor's thesis, University of Twente.

[14] Zinno, S., Di Stasi, G., Avallone, S., Ventre, G. (2014). A load balancing algorithm against DDoS attacks in beyond 3G wireless networks. In 2014 Euro Med Telco Conference (EMTC), Naples, Italy, pp. 1-6. https://doi.org/10.1109/EMTC.2014.6996647

[15] Do, T.N., Tran, P.T., Le, H.T. (2021). Study the coexistence NB-IoT paging and LTE paging on eNodeB. In 2020 IEEE Eighth International Conference on Communications and Electronics (ICCE), Phu Quoc Island, Vietnam, pp. 80-84. https://doi.org/10.1109/ICCE48956.2021.9352146

[16] Hara, K., Shiomoto, K., Eng, C.L., Backstad, S. (2020). Automatic enodeb state management in lte networks using semi-supervised learning with adversarial autoencoder. In 2020 IEEE 21st International Conference on High Performance Switching and Routing (HPSR), Newark, NJ, USA, pp. 1-6. https://doi.org/10.1109/HPSR48589.2020.9098982

[17] Djomadji, E.M.D., Kabiena, I.B., Nkemeni, V., Njere, A. G.B.À., Sone, M.E. (2023). Dynamic resource allocation in LTE radio access network using machine learning techniques. Journal of Computer and Communications, 11(6): 73-93. https://doi.org/10.4236/jcc.2023.116005

[18] Jeon, D., Tak, B. (2022). BlackEye: Automatic IP blacklisting using machine learning from security logs. Wireless Networks, 28(2): 937-948. https://doi.org/10.1007/s11276-019-02201-5