DDoS Attack Identification

Utilizing Machine Learning in Circumstances Involving Hacked IoT Devices/Insider Assaults

2022-03-17

Authors:

Rani Yadav-Ranjan
rani.yadav-ranjan@ericsson.com
Global Artificial Intelligence Accelerator, Ericsson

Arthur Brisebois
arthur.brisebois@ericsson.com
Global Artificial Intelligence Accelerator, Ericsson

Serene Banerjee
serene.banerjee@ericsson.com
Global Artificial Intelligence Accelerator, Ericsson

CONTENTS

FIGURES

1 OVERVIEW

Internet of Things (IoT) device density/volume is the new Distributed Denial of Service (DDoS) risk for 5G. The utilization of cloud and edge computing, as well as the convergence of mobile and traditional IT networks, results in the creation of powerful new attack vectors for IoT applications and networks. The challenge is to convert the risk of high-volume IoT attacks to an opportunity to observe and steer a larger sample of IoT devices and nodes involved in potential attacks. An additional challenge is to convert complexity, of distributed networks, to additional DDoS detection and countermeasure horsepower.

Another key challenge is to convert radio network complexity and DDoS vulnerability to even more powerful DDoS detection and countermeasure horsepower. Diversified DDoS detection and countermeasures are therefore crucial for IoT applications and the networks that host them. Emerging technologies, such as blockchain and smart contracts, enable the fully distributed and automatic exchange of attack information. This paper investigates how 5G radio networks and blockchain can be used in tandem to provide an additional layer of protection against IoT DDoS attacks.

1.1 INTRODUCTION[1]

The challenge of detecting DDoS attacks is not entirely new, but when high IoT device density is considered, the scale and associated automation needs are. We propose a step-by-step approach for DDoS detection as described below:

- **Sensing**: We must first identify which measurement points and metrics can reveal a potential DDoS attack. Examples include UE trace and/or billing records, radio eNB / gNB, MME / AMF for control plane sensing, and PGW / UPF for user plane sensing.
- **Baseline state models**: We must next build models which represent "normal" or non-anomalous UE and network states, observe-able by sensing, that exist before the DDoS incident. Examples include UE volume / attach / tracking area update per hour, radio uplink noise, RACCH occupancy, MME / AMF attach / tracking area update per attached UE / hour, and PGW / UPF data volume per connected UE.
- **Network and UE anomaly detection**: We must next begin with a means to detect an abnormal condition, which may or may not be DDoS, from available UE and network sensing data which is out of alignment with baselines. Anomaly examples include uplink noise, signaling, and/or user data traffic volume spikes compared to baseline.

[1] U.S. Patent pending No. 63/307,519.

- **Network and UE anomaly classification**: Once detected, anomalies must be classified prior to causal inference and other steps. This classification is needed in order to narrow relatively broad, and compute expensive, causality inference actions to a manageable set. Sensed data patterns are temporal, spatial and distribution clues that suggest an optimal path for causality inference.
- **Network and UE causality inference**: The combination of network and UE anomaly classification should be used to initiate/instantiate a targeted causality inference path.
- **Network countermeasures and remedial actions**: Once classified, UE and network DDoS causes must be addressed via countermeasures and remedial actions. If coordinated / coincident UE signaling actions are observed, then appropriate countermeasures must be instantiated to steer these UE down a network path which limits their impact on the upstream network and legitimate UE. In this case, a desirable outcome may be for the anomalous UE to impact or deny service to each other, thus using the high density of DDoS IoT devices as an enabler, versus challenge, to a powerful DDoS defense mechanism. Next, additional spatial classification, using geolocation techniques, should be used to identify the presence or absence of DDoS device clusters. Additional remedial actions, including automated over-the-air software updates, may be used to further identify, repair, impair or completely disable DDoS devices. Finally, proactive actions must be taken to prevent DDoS UE from impacting additional networks after detection. These countermeasures and remedial actions should all be designed to mimic normal or DDoS-impaired conditions that are difficult for IoT devices to detect or counter.

1.2 STRUCTURE

The document is organized as follows:

- Chapter 2 – Motivation
- Chapter 3 – Distributed DDoS Attack Detection
- Chapter 4 – DDoS Countermeasures
- Chapter 5 – Summary and Next Steps

1.3 TERMS AND DEFINITIONS

The following terms and definitions that are key to understanding this document are:

- 5G – Fifth-generation technology standard for broadband cellular network
- AMF – Access & Mobility Management Function
- ARFCN – Absolute radio frequency channel Number
- DDoS – Distributed Denial of Service
- DIU – Data Interface Unit
- DTW – Dynamic Time Warping
- EARFCN – E-Ultra Absolute Radio Frequency Channel Number

- Edge-IoT – Point where data is collected, sensing is done for Internet of Things device
- eNB – Base stations in 4G LTE networks
- gNB – 3GPP 5G next-generation base station supporting 5G
- HMM – Hidden Markov Models
- IMEI – International Mobile Equipment Identity
- IoT – Internet of Things
- KPI - Key Performance Indicators
- LTE – Long-Term Evolution
- MEC – Multi-access Edge Computing
- MME – Mobility Management Entity
- PGW – Packet Data Network Gateway Technology
- RACCH – Random Access Control Channel
- RACH – Random Access Channel
- RAN – Radio Access Network
- RL – Reinforced Learning
- RRC – Radio Resource Control
- SINR – Signal to Interference Plus Noise Ratio
- Slice – Independent end-to-end logical network
- STFT – Short Time Fourier Transform
- UE – User Equipment
- UPF – User Plane Function
- Uplink – Part of the communication link signal

2 MOTIVATION

By 2027, IoT devices are expected to outnumber mobile phone devices by a factor of nearly 4 to 1. Through efficiency and capacity upgrades, 5G IoT devices and radio networks are likely to absorb a large portion of this demand rise. While the radio interface will eventually become less of a bottleneck for legitimate IoT device and traffic volume growth, it may also pass on a greater number of illegitimate IoT DDoS attack traffic to upstream network nodes and IoT platforms.

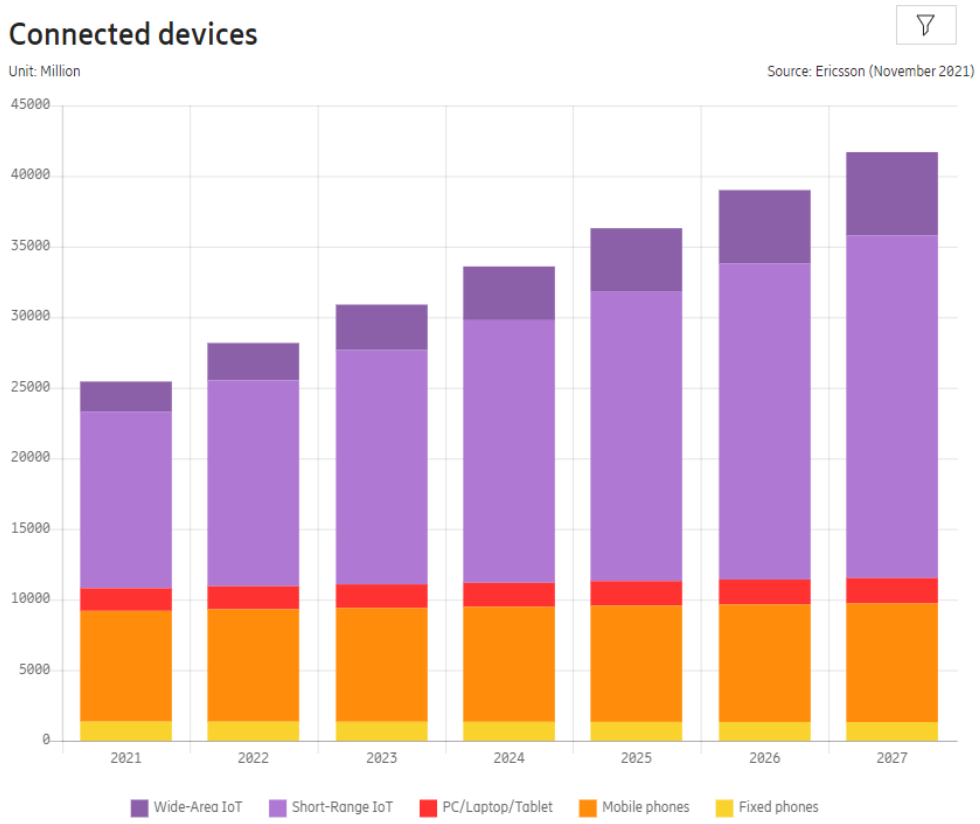

Figure 2-1: IoT connected device forecast.

Most IoT devices lack a user interface to observe UE behavior, accept software updates and other human-enabled oversight applied to mobile phones. This, plus the sheer number of IoT devices, drives the need for mechanized IoT device management platforms. Such automation enables scale but presents a risk if a single compromised device management platform can rapidly deploy faulty or malicious software to a massive number of IoT devices.

Legacy DDoS detection, countermeasure, and mitigation mechanisms, designed for mobile phone networks, will therefore be unable to handle the pace and intensity of automated IoT DDoS attacks. The risk of such massive automated IoT DDoS attacks drives the need for intelligent, automated network DDoS detection, countermeasure, and mitigation mechanisms.

2.1 Motivation for the Use of Radio, Machine Learning and Blockchain Technologies

Much progress has been made with DDoS detection and countermeasures for traditional IP networks. We aim to address incremental vulnerabilities and opportunities associated with DDoS attacks over wireless networks serving IoT devices. Traditional DDoS detection mechanisms (for example ieeexplore.ieee.org/document/9246616: April 2021) detect and classify DDoS through IP flow observation from a central cloud platform connected to network core nodes. As wireless

network flows become more distributed, to satisfy IoT performance and scale requirements, they also become more difficult to monitor from a central cloud platform. Central IP flow transportation and processing, for DDoS detection, will be difficult to scale and secure.

Distributed, blockchain-based DDoS detection and defense approaches (for example *https://hal.inria.fr/hal-01806063*: Jul 2017) propose use of Blockchains to detect and report DDoS via Smart Contracts deployed at various distributed network nodes along the IP path to the victim server. These methods certainly address some of the aforementioned user plane IP flow transportation and processing scale-ability and security concerns, but they do not observe cellular network radio and control plane DDoS attacks.

Traditional and proposed DDoS defense mechanisms, including the central and Blockchain distributed examples described above, suggest detection and mitigation mechanisms that address and defend against DDoS attacks of servers through an instrumented IP network. These traditional defense mechanisms, including IP blacklisting, packet dropping and connection rejection, protect the victim server, but they fail to protect the network radio or control resources along the path. Section 5 describes scenarios where some traditional defense mechanisms may exacerbate / amplify network radio and control resource attacks.

In summary, we aim to fill gaps in existing detection and countermeasure mechanisms that lack the scale and radio awareness to address the wireless IoT DDoS threat. Our solution includes radio and Blockchain DDoS detection techniques that complement radio countermeasure techniques.

3 Distributed DDoS Attack Detection

During an IoT DDoS attack, potentially massive number of IoT devices initiate an abnormally high volume of various transactions towards a destination. These excess transactions may intentionally or unintentionally cause congestion and instability at the destination and / or various intermediate nodes and interfaces along the path between the origin (radio) and the destination (server). We propose a distributed detection approach that yields DDoS detection alerts closest to the source(s) and time of attack.

3.1 Radio DDoS Detection

All wireless IoT transactions, legitimate and illegitimate, begin with radio network access. Each radio network access attempt includes IoT UE uplink radio transmissions that yield useful signal, for the intended transaction, and noise interference for all other transactions sharing the same cellular frequencies. IoT DDoS attacks may lead to a rise in uplink noise in the serving cell, but not in the neighboring cells nearby.

This is because high-volume, low cost IoT devices typically have low transmitter and battery power and are more effective for DDoS attacks close to the victim cell site. Legitimate UE traffic is typically dispersed over larger areas between multiple cell sites. If the noise is from typical

legitimate traffic, the neighbor cells are also likely to experience a similar rise in uplink noise. In the case of a DoS attack, the noise rise is local to that cell under consideration only, with minimal environmental impact. The same is depicted in Figure 3-1, with average interference of the primary cell (in red), the average SINR of the primary cell (blue), and the average interference of the first neighbor (green).

It can be seen that the rise in uplink noise of the primary cell follows a pattern very similar to that of its neighbors and can be seen for most of the days – this is clearly due to typical legitimate traffic. On the second day, the rise in noise exceeds that of the neighbors and there is little or no environmental impact. Here, we observe the following:

a) Uplink noise is low and similar to neighbor cells most of the time
b) There are traffic-dependent spikes in uplink noise that are higher than neighbor cells, and
c) Uplink SINR drops do not correlate with uplink noise rise at neighbor cells, i.e. it is local traffic-dependent noise with no environmental impact
d) Some connected UE exhibit signaling and/or user data volume patterns that correlate with the uplink SINR patterns of the attacked cell. These UE are classified as DDoS perpetrators.

Hence, it is possible to conclude that the uncorrelated noise is from DoS. We propose time series-based anomaly detection to detect the same, as discussed below.

The data for this work was obtained from 50,000 cells collected from a customer LTE network. The Key Performance Indicators (KPIs) were collected at every 15 minutes. The KPI that is primarily used for this work was Radio interference in the control and shared channel for each cell and it's 3 neighbors. The neighbors were decided based on the number of handovers or using the cell latitude/longitude.

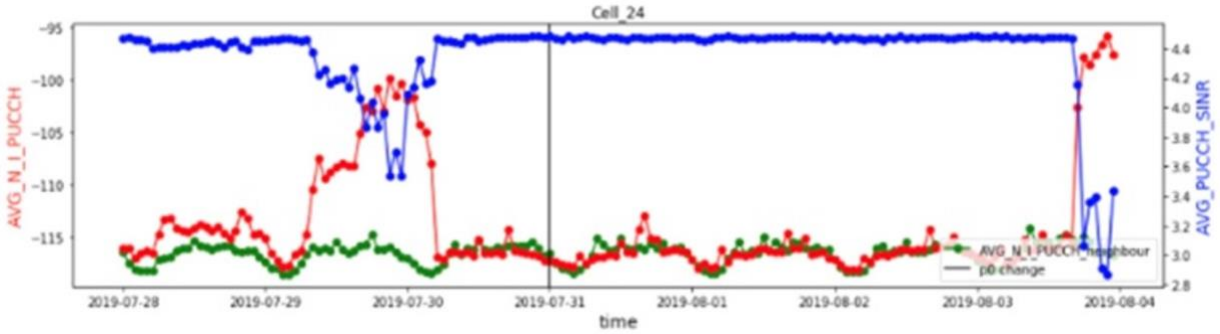

Figure 3-1: Rise in Uplink noise due to DoS may not have an impact on the neighboring cells. In blue is SINR of primary cell, and in red the interference of primary cell. In green, is shown the interference of the first neighbor.

3.2 ENSEMBLE-BASED APPROACH

For radio DDoS detection, we must exploit temporal and spatial observations from multiple radio nodes. We propose an ensemble of time series-based machine learning and signal processing approaches, that can automatically identify DoS in real-time, by analyzing Key Performance

Indicators (KPI) of the primary cell and its nearest neighbors. We validate our results for various environmental conditions in data available from LTE and 5G consumer networks. We propose a combination of:

a) Time series distance-based measures, such as Dynamic Time Warping (DTW),
b) Frequency domain-based measures or generalized (uniform or non-uniform) filter-bank based approaches, such as Wavelets and Short Time Fourier Transform (STFT), and
c) Sequence model-based measures, such as Hidden Markov Models (HMM).

The block diagram of our approach is shown in Figure 3-2.

We further have extended the work to multi-frequency time series, by using Fourier Feature Mapping to handle finer time granularities and detect DoS anomalies in an online learning setting.

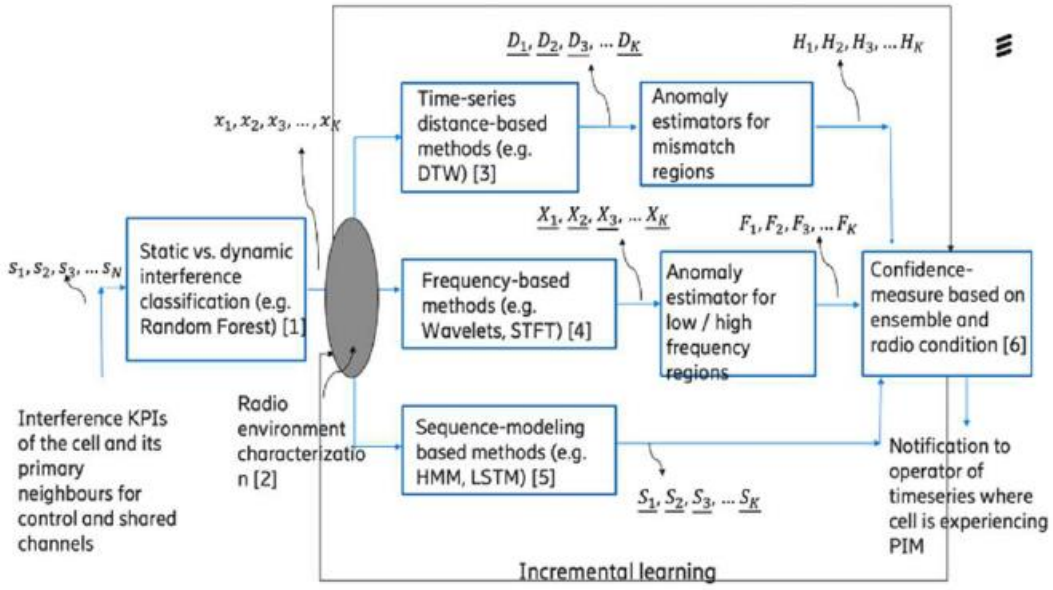

Figure 3-2: Block-diagram of the ensemble-based approach for time series ensemble-based approach for network anomaly detection under DoS attacks.

3.3 Self-Supervised Learning-Based Approach

We further propose a self-supervised reinforcement learning approach to predict DoS-related anomalies before they occur. Such predictions may, for example, observe the leading edge of a large-scale IoT DDoS attack, and initiate countermeasures before the entire local population of IoT devices join the attack. We forecast environmental conditions that give rise to DoS based on offline historical data and models that predict future occurrences. T

These approaches were tested on customer LTE data for 50,000+ cell sites. The Key Performance Indicators (KPIs) were collected at every 15 minutes. As a DDoS attack is correlated to a rise in uplink noise in the primary cell, and not in the neighbors as described above, we mark the rise in

uplink noise as an anomaly. The block diagram of the self-supervised anomaly detection from uplink noise rise is shown in Figure 3-3.

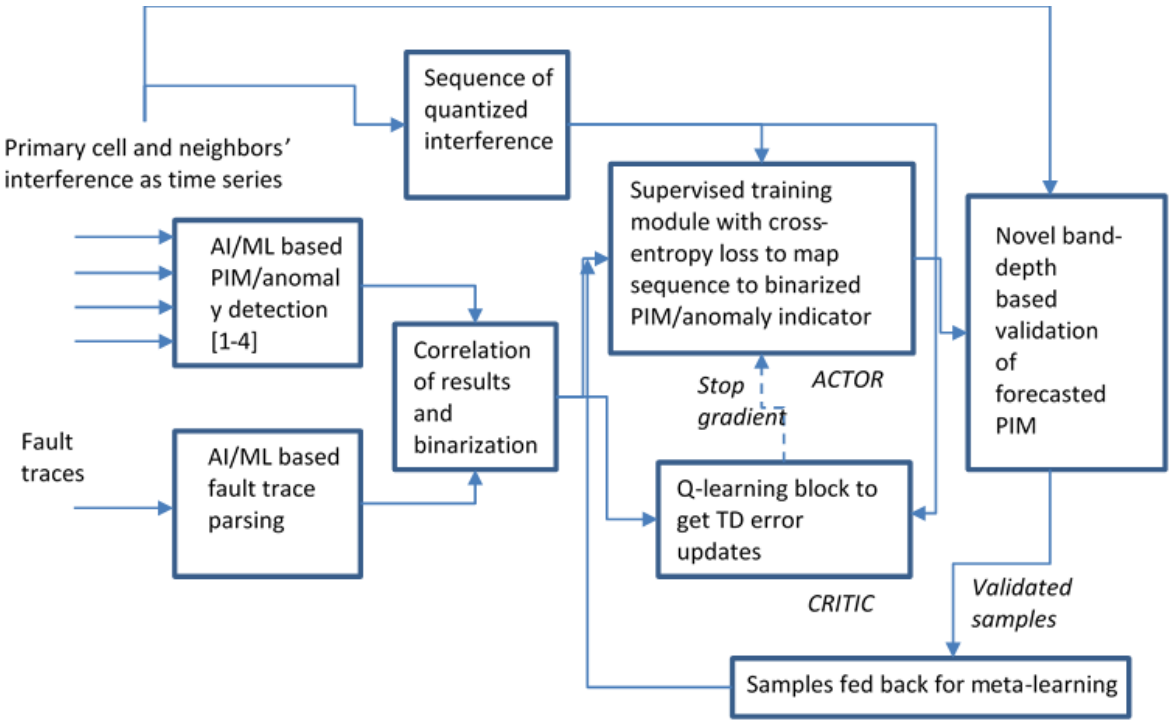

Figure 3-3: Block diagram of the self-supervised approach for anomaly detection from uplink noise rise.

We can then formulate the next occurrence of an anomaly as a Markov Decision Process (MDP), where state, action, and rewards are as described below:

a) **State:** In our case, the state is the quantized values of sequential interference that the cell is experiencing. Higher interference could lead to call drop, service degradation, etc.
b) **Action:** Actions are quantized interference values that led to a positive affirmation of the presence of an anomaly.
c) **Reward:** The reward can be defined as per domain knowledge. Reward is dependent on Radio Access Networks (RAN) KPI values and their thresholds. Some of the important RAN KPIs that we have considered identifying anomalies are CDR (call drop rate), CSSR (call set-up success rate), HSR (handover success rate), TCH (traffic channel congestion rate), call completion rate, speech quality index & signal strength. e.g., if the signal strength is below threshold i.e., signal strength is not falling between the required dBm range then reward will be positive as interference leads to poor signal strength.

Depending on the "action", the reward can be either positive or negative. Reward is positive if interference is observed and negative if there is no interference at that state. For example, it is known that anomaly will be prominent for cells to experience higher traffic. So, traffic could be a trigger to give more reward. To promote recommendation diversity, in addition to traffic other factors that can be considered, include but are not limited to, path loss, time of the day, etc. The

RL-agent then tries to maximize the expected cumulative reward. In this learning setup, the self-supervised Q-learning loss is defined as a cross-entropy loss. The cross-entropy loss is used to rank the sequence of events to a binarized indicator of the occurrence or absence of the anomalous event. This cross-entropy loss measures the performance of a classification model where the output may be a probability value between 0 and 1. For example, an anomaly may be a 1, and a non-anomaly may be a 0. Then, via a neural network, may now generate probability values between 0 and 1, to match the training data. If a value is 0.02 at a place where it is 1, it may give a high loss value. A perfect model may have the cross-entropy loss to be 0, that is, e.g., that the 1 may be predicted as 1. The self-supervised reinforcement learning module may then learn patterns in the data that may potentially give rise to local anomalies.

For the actor-critic variation, the self-supervised head is the “actor”, and the Q-learning module is the “critic”. The self-supervised learning network may be used to determine which factors to give more weightage to in the predictive model. Factors or features are combinations of variables that may give rise to an anomalous event, e.g., combinations of KPIs, such as interference, load, atmospheric conditions, etc. The training loss of the approach versus the epochs is shown in Figure 3-4.

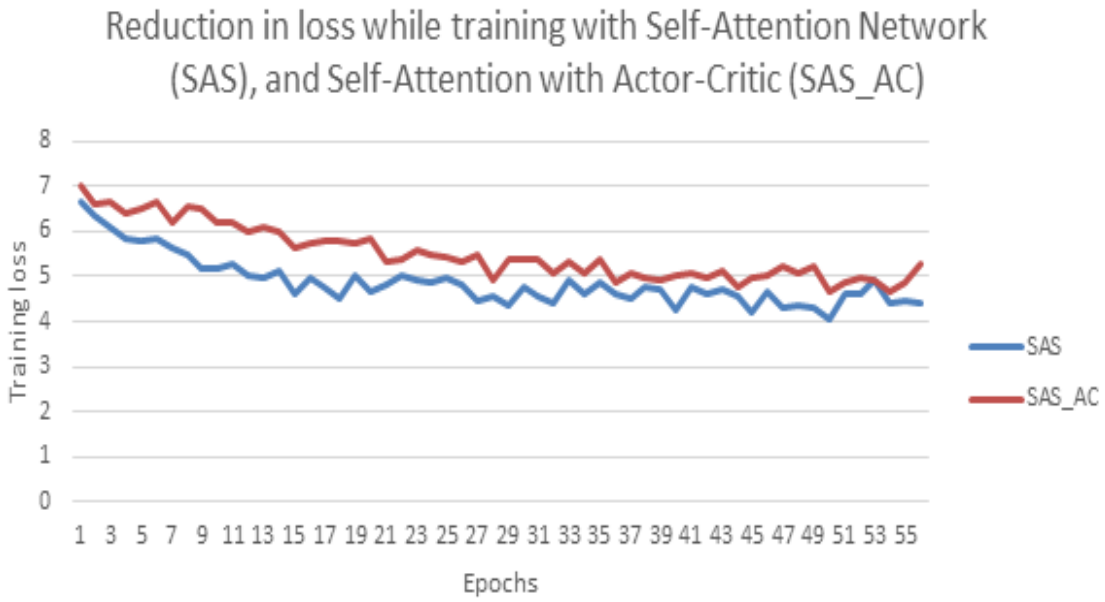

Figure 3-4: Decreasing loss of the self-supervised actor-critic method for anomaly detection.

3.4 Analysis and Results

Based on the above modeling, experimental results from this real-world dataset have been shown to accurately predict noise rise 60% of the time, before it is strong enough to deny service. This ensures that we can instantiate other anomaly detection, causality, and countermeasures before the IoT DDOS has achieved full effect. To the best of our knowledge, this is the first work where DDOS anomalies are predicted and countered before they occur.

3.5 CORE DDOS DETECTION USING BLOCKCHAIN

Beyond the radio, IoT transactions disperse between control and user plane core nodes along the path from the IoT device to the server. Each IoT transaction involves multiple network control plane nodes, that manage IoT device to radio network coordination, and network user plane nodes, that manage IoT device to server data packet transportation. These core nodes are interdependent DDoS victims and detection points.

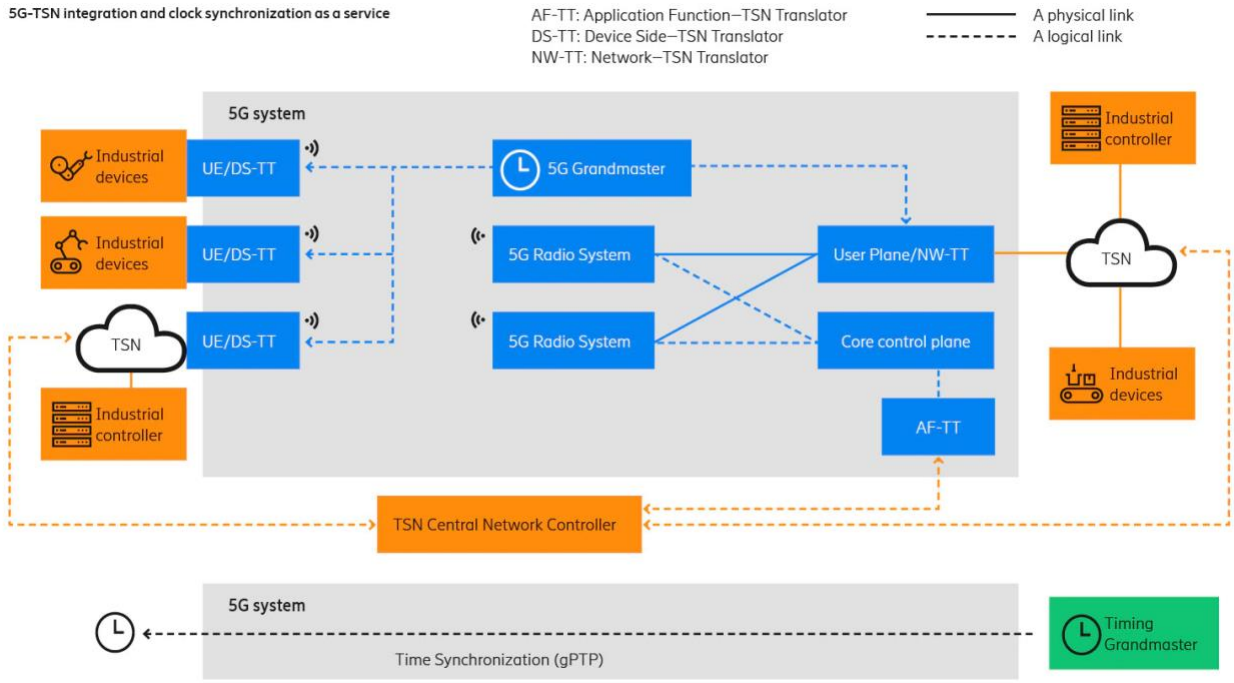

Figure 3-5: High-level IoT network topology.

As is true for radio, core node DDoS detection must exploit temporal and spatial observations from multiple core nodes. Sensing data must be compared at multiple nodes (including virtual functions and their host locations) in order to determine if anomaly trends occur at the same time, with perhaps different intensities. If yes, then common spatial and morphology factors, for example overlapping or adjacent coverage areas and host locations, must be identified. If no, then node-specific indications, including metrics and alarms, should be observed for temporal correlation to the anomaly condition.

Such observations should lead to a distributed or local network anomaly classification. From the UE / subscriber perspective, sensing data must be analyzed to determine if network-observed anomalies correlate with signaling spikes for a single UE or multiple UE with something in common. Such observations should lead to a distributed or unique anomaly classification or some sort of distribution factor shades between "black" and "white".

If network and UE anomaly classifications are distributed, then network and UE sensing data must be observed for temporal relationships to determine if a large number of UE affected a large number of network nodes (DDoS), or a large number of network nodes affected a large number of UE (network failure).

If network anomaly classification is local and UE anomaly classification is distributed, then an inverse correlation study of UE sensing data can determine what is different, for example, virtual RAN and core network functions and hosting locations, between UE with and without anomalous behavior in the same RAN area. If network anomaly classification is distributed, and UE anomaly classification is relatively unique, then UE sensing data should be observed for coincident behavioral patterns of multiple UE. For example:

a) Do all anomalous UE exhibit signaling spikes at the same time on different virtual core nodes connected to the same RAN?

b) What happens to the signaling volume of non-anomalous UE on the same RAN nodes as anomalous UE?

c) What is the difference between the anomalous and non-anomalous UE (subscription/slice, IMEI range indicating hardware)?

d) What is common between the anomalous UE? For example, do they all change cells at the same time, indicating the presence in a common vehicle, etc.

Layers of anomaly classifications and causal inference should lead to targeted UE or network remedy actions.

The challenge is to observe and act on data, from all the distributed core nodes, without creating an unmanageable amount of data collection, transportation, privacy and compute overhead. Blockchain is a new technology that records and maintains transactions in a verifiable and permanent manner using decentralized and open ledgers that can be updated from multiple nodes along a network transaction path.

A smart contract is a computer program that is executed in a secure environment that directly monitors and controls digital assets. A smart contract can be configured with rules that update records when specified conditions are met at nodes along a network transaction path.

As shown in Figure 3-6, when applied to the IoT DDoS use case, blockchain records and smart-contract-initiated updates can be used to track device behavior and network impacts, and therefore provide an efficient data source for DDoS anomaly detection, countermeasure, and mitigation functions, from each intermediate node. Compared to traditional probing, packet inspection, and data caching techniques, this blockchain approach is better suited for the privacy, scale, and speed of IoT networks.

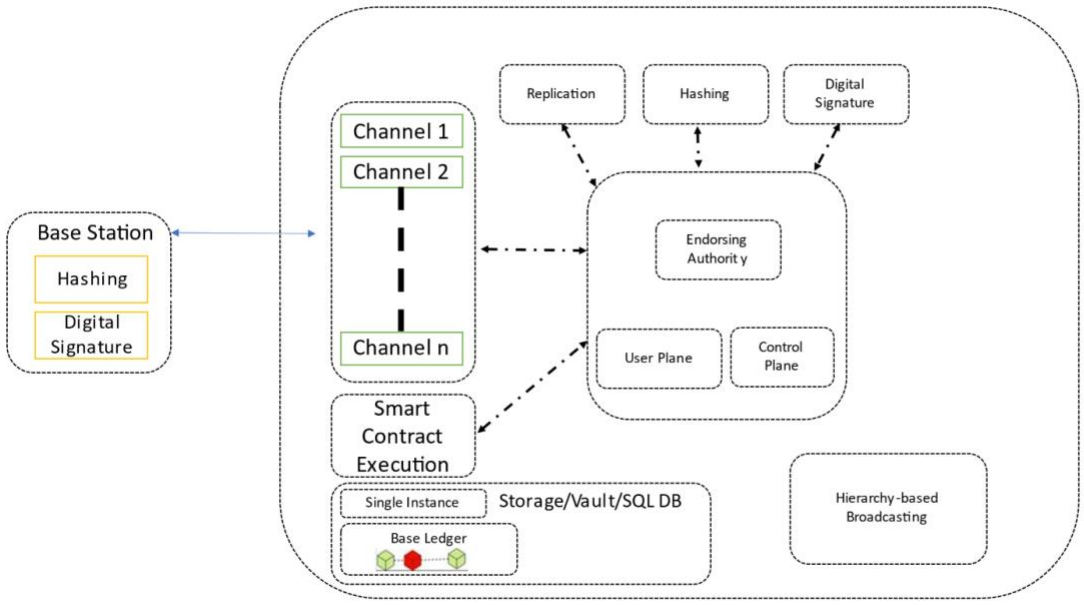

Figure 3-6: The process used for Smart Contract recording DDOS threats and countermeasures.

Applied to control plane nodes, blockchain smart contracts can observe and alert anomalous UE detach, reconnect, paging, location update, and re-establish behaviors that indicate control plane DDoS attacks. Applied to user-plane nodes, blockchain smart contracts can observe and alert anomalous packet flow volume and activity patterns that indicate user plane IoT DDOS attacks. When combined from multiple nodes serving the same devices, blockchain smart contract reports can be observed for temporal and spatial patterns that can point to the presence, origin, and destination of DDoS attacks. Application of blockchain records and smart contract induced updates to IoT DDoS use cases provides an effective distributed data source for DDoS anomaly detection, countermeasure, and mitigation functions. Blockchain-based solutions are better suited to IoT networks than classical probing, packet inspection, and data caching techniques because the raw data and rule computations are handled at the distributed nodes.

Opportunities include:

(1) **Distributed nodes that are scattered**. The transition from centralized cloud computing to decentralized Edge computing is well-suited to the decentralized Blockchain. Running Blockchain among distributed nodes has the potential to enable safe data sharing, tracking, and validation for large-scale IoT applications. As DDoS packets (user data or signaling data) traverse multiple distributed edge and internal nodes and interfaces, they can be observed and selectively identified by smart contracts at each distributed node. This is analogous to trapping fish at the incoming stream, versus angling the entire lake. When compared to centralized commercial clouds, the operational expenses of Blockchain and smart contracts could be greatly lowered.

(2) **Interaction between IoT devices and distributed nodes**. Many problems with IoT devices can be solved using blockchain and smart contracts. If / when DDoS attacks are successful, they may create logjams (extra transaction volume and latency) at impacted nodes and interfaces. If these nodes and interfaces each have smart contracts with transaction volume and latency rules, then we'll get reports on when and where the logjams occur. Sensing DDoS anomalies at the source is, therefore, more time and cost-efficient than mining anomalies from a central data lake.

(3) **Resistance to IoT cyberattacks**. IoT devices typically lack the resources or capabilities to perform full-fledged security processes in the face of threats. - Lightweight security approaches may be useful, but they are still in their infancy. Hackers will find it far more difficult to disrupt the Blockchain without having enough CPU power to outrun the combined CPU power of the entire network and without being discovered with Blockchain and decentralized ledgers. Node based Smart contracts also allow IoT devices to define agreements on specific actions, behaviors, and results, allowing hackers' anomalous conduct to be spotted, detected, and reported automatically. Furthermore, with the trusted Blockchain, it is feasible to set a "zero-trust" policy in the distributed network, which might monitor all network transactions and aid in the detection of strange behaviors, potential misuses, and assaults. Without being noticed and stopped, lateral moves from the hackers to the attacking targets will be far more difficult.

4 DDoS Countermeasures

Deception-based defense is an effective cyber defense strategy which employs a variety of techniques to deceive, perplex, and apprehend dangerous hackers. Address hopping, network telescopes, and honeypots are examples of common methods. Radio networks are vulnerable, yet uniquely equipped to locate and apply covert radio countermeasures for IoT DDoS attacks.

4.1 DDoS Location Fingerprinting

Numerous radio DDoS mitigation and remediation procedures can be targeted at specific locations and cell sites. This targeted strategy will be enabled by the location fingerprinting of DDoS UE and the possibility of "swarms" of DDoS UE. While active, all cellular UEs adjust their uplink transmit burst timing to align with the frame structure of the serving cell site receiver.

As each UE moves further away, uplink transmits bursts take longer to reach the cell site. When the reception is delayed beyond a threshold, the cell site commands the UE to increase the timing advance value, thus sending uplink bursts sooner to overcome the additional delay. Each timing advance increment represents a 78M distance between the UE and cell site.

When classified as DDoS, the timing advance value can be used to geolocate the perpetrator UE within a 78M band around the known cell site location. When there are handovers between two cell sites of known location, the old (before handover) and new (after handover) timing advance values can be used to narrow the location estimate even further. If there are handovers between

three or more cells in a constellation, as per cells 1, 2, and 3 below, the location estimate can be reduced to a 78M diameter circle.

If multiple DDoS perpetrator UEs affect the same cell site at the same time, they may be clustered together in a van or building that can be investigated by law enforcement. In this case, a time series of cell site and timing advance changes can be observed and compared for each suspect DDoS perpetrator UE. If cell site and timing advance changes for multiple DDoS perpetrator UEs coincide, then these perpetrator UEs are likely in the same moving vehicle or building.

If suspect DDoS perpetrator UEs are stationary for a considerable time, then the radio network can force handovers while observing timing advice values between neighboring cells in a constellation such as C1, C2, and C3 in Figure 4-1 below.

This technique can also be enhanced by the angle of arrival data where beamforming radios are deployed. If all perpetrator UEs align with the same 78M diameter circle, they, and their operator, are likely in the same location.

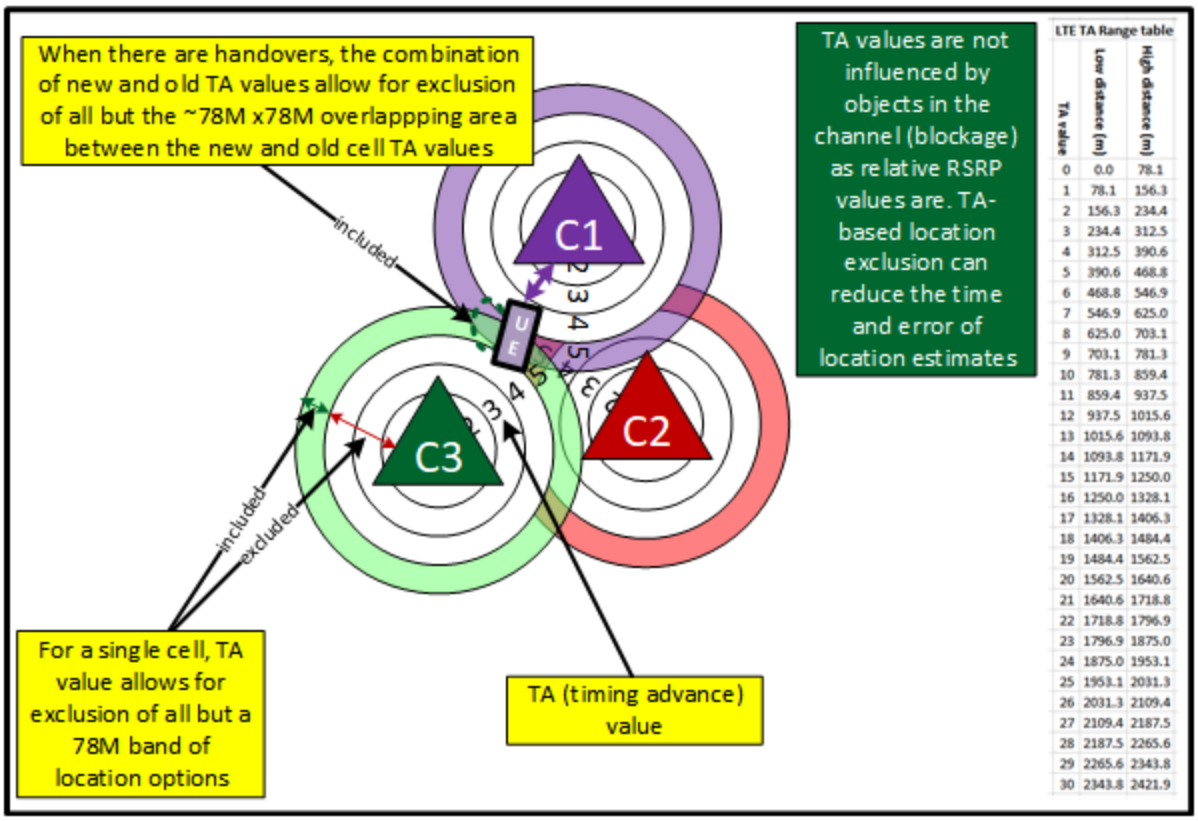

Figure 4-1: Timing Advance (TA) for DDoS location fingerprinting.

4.2 Covert Radio Countermeasures for DDoS

In Section 3.1, we describe radio noise pattern observation as a means to detect and classify the presence of over-the-air DDoS attacks and perpetrator UEs from cell sites. In Section 3.2, we

describe use of Blockchain Smart Contracts to detect and classify control and user plane DDoS attacks from network core nodes. In Section 4.1, we describe timing advance observation to form a location fingerprint for perpetrator UEs involved in over-the-air DDoS attacks. The next challenge is to minimize or preferably eliminate the DDoS impact of IoT devices classified and localized as perpetrator UEs in a specific area. As per Figure 4-2, DDoS attacks may target one or many networks, platforms, applications, or service victims.

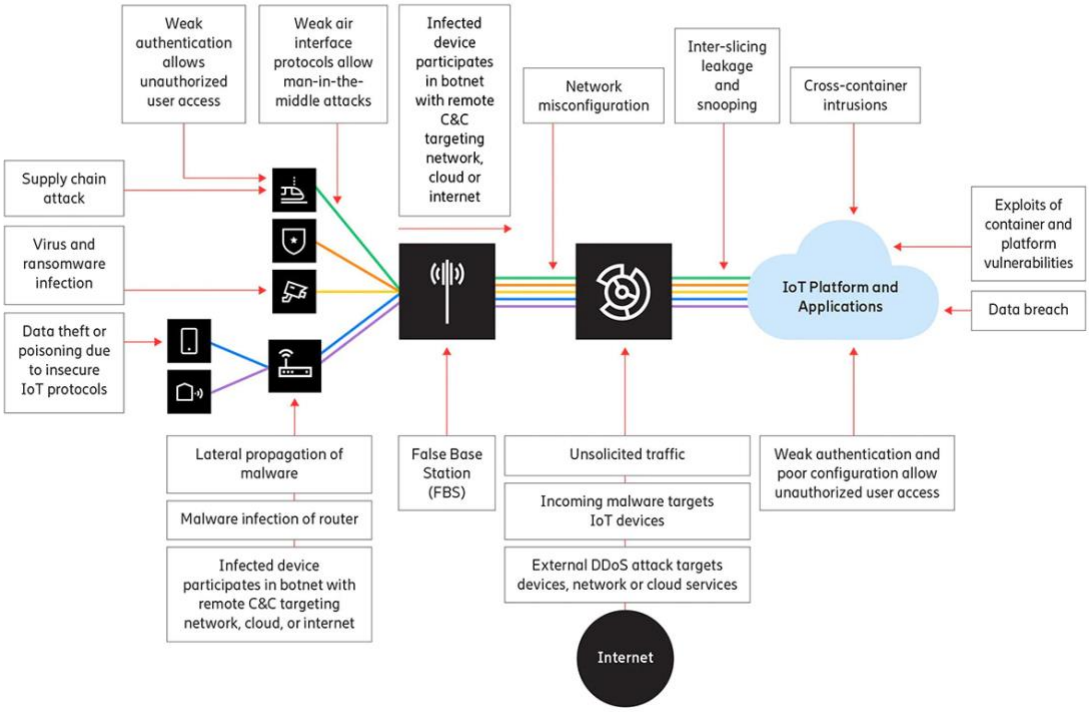

Figure 4-2: IoT security threat environment.

Considering the variety and the sheer number of IoT devices and DDoS victims, it is relatively impractical and/or ineffective to apply countermeasures and mitigation at all endpoints and intermediate nodes. Some intermediate node mitigation techniques may even exacerbate DDoS impact for other nodes in the network. For example, packet core nodes may selectively drop packets for DDoS perpetrator flows, thus rate-limiting the DDoS impact to upstream nodes in the core, internet, and IoT platforms.

This kind of overt countermeasure action will trigger an even more damaging reaction, packet retransmission, from the perpetrator UEs. Packet retransmission will amplify the radio noise and congestion that triggered DDoS countermeasures and mitigation in the first place. Another intermediate node DDoS mitigation technique, called “defense by offense”, deliberately increases the volume of “good client” traffic so there is less bandwidth for the DDoS perpetrators to use.

This method may slow down the DDoS devices, but it will also amplify radio noise and congestion that triggered DDoS mitigation in the first place. Traditional radio congestion mitigation techniques, such as RRC connection reject, may also amplify DDoS radio degradation. In the RRC connection reject case, the victim cell sends RRC connection reject, along with a wait timer ranging from 0 to 16 seconds to the DDoS perpetrator UEs. This kind of overt countermeasure action may cause the compromised perpetrator UEs to ignore wait times and instead send noise inducing RRC requests at an even faster rate.

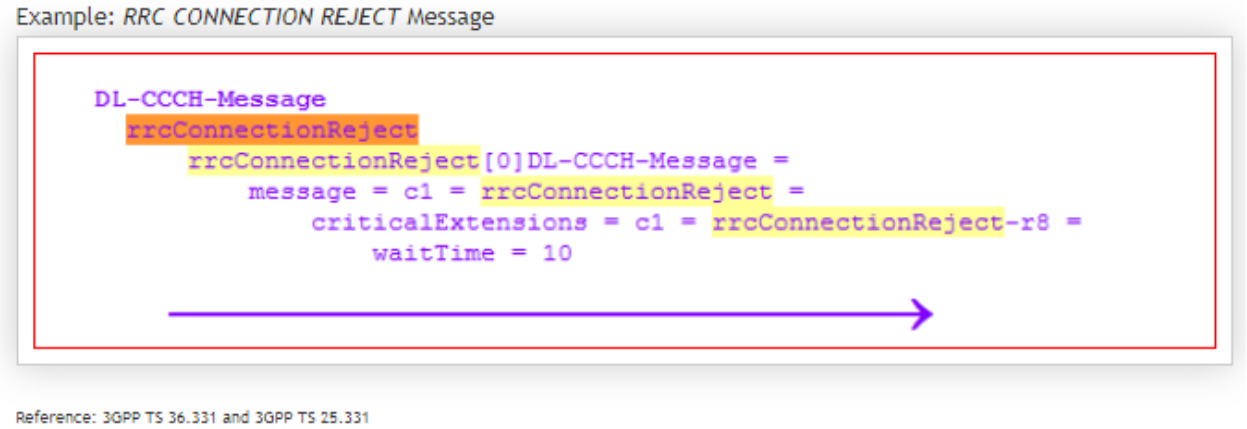

Figure 4-3: RRC Connection Reject message per 3GPP TS 36.331.

Considering these examples, IoT device density, and the sheer volume of DDoS attacks they could bring, a more targeted yet less overt radio countermeasure and mitigation approach is required.

According to 3GPP 38.300 standards, all UE, including IoT, must initially access the radio network via a Random-Access Control Channel (RACH). For each UE, this shared RACH is the initial path to dedicated resources used for the remainder of any transaction. While sharing a common primary cell (radio carrier), UEs must share and therefore compete for RACH resources in a contention-based or contention free manner.

In contention-based RACH, over-active DDoS UEs may jam the RACH with interference in the form of RACH collisions with other UEs attempting to access the same cell at the same time. In contention-free RACH, over-active DDoS UEs may occupy a disproportionate share of RA preamble assignments. In either case, legitimate UEs, sharing the same RACH with DDoS UEs, will suffer delayed or blocked access to the radio network.

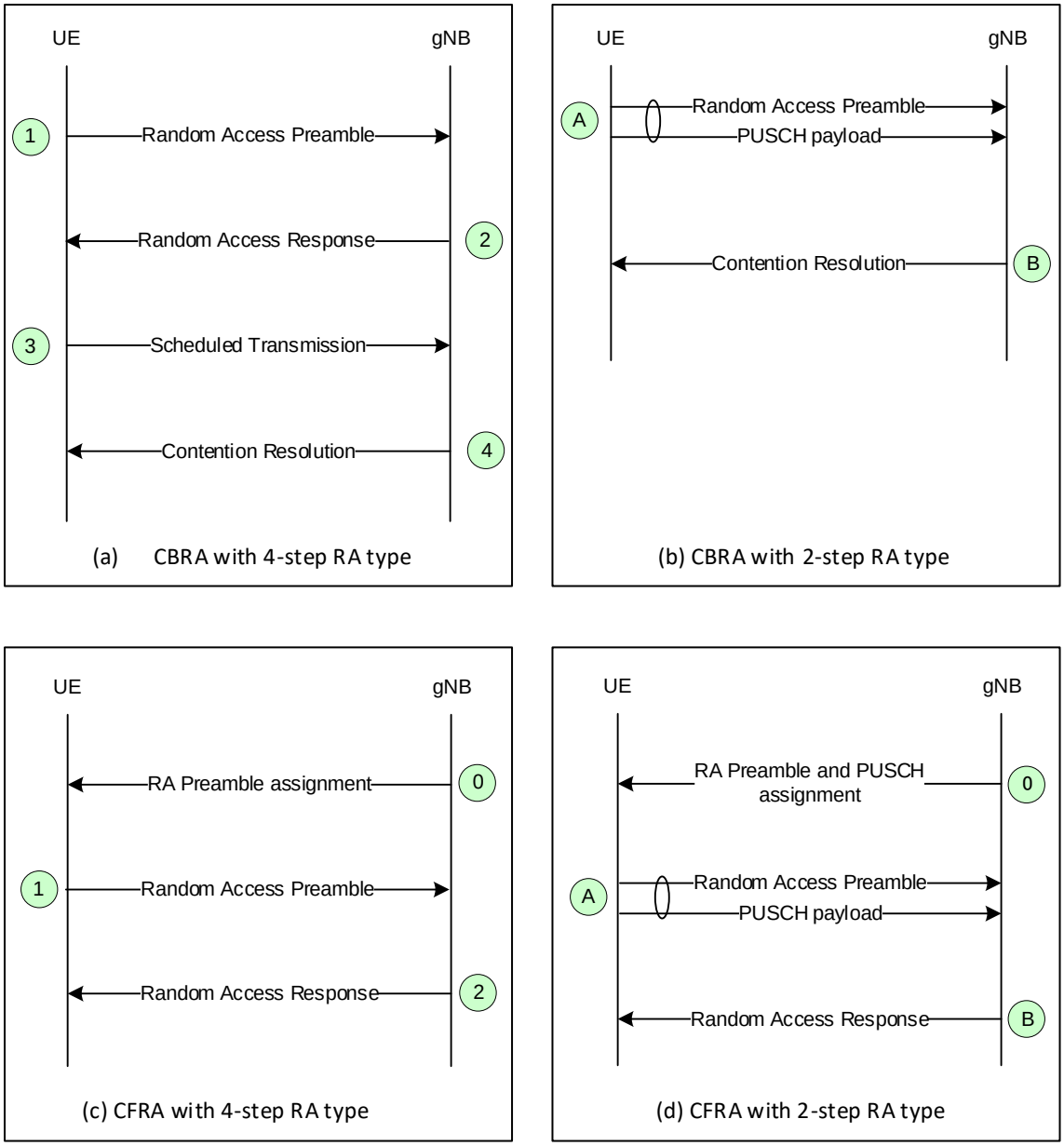

Figure 4-4: Contention-based and contention-free RACH procedures.

Under typical load conditions, all UEs are load balanced between available frequencies and RACH resources. This is accomplished with inter-frequency handovers at the leading edge of transactions, and/or release with cell info at the trailing edge of transactions. Such load-balancing behavior is optimal under normal conditions, but with DDoS, this approach multiplies the legitimate UE impact and radio RACH signaling capacity between DDoS UEs and upstream targets.

When DDoS is detected, the cell site applies a defensive load balance mechanism which pushes DDoS UEs towards a single, narrow radio frequency that is not shared with legitimate UE. This is accomplished via assignment of a DDoS countermeasure SPID (Service Profile Identifier), which narrows DDoS UE access to a single selected radio frequency.

In cases, such as private networks, where available spectrum is initially applied to a single radio frequency (ARFCN or EARFCN), the cell site may subdivide the spectrum by creating two new frequencies with imbalanced bandwidth. Over-active DDoS UEs compete and collide with each other for fewer RACH resources on a single, narrow radio frequency, and are less likely to acquire dedicated resources towards the upstream network, platform, application, and service nodes.

From the DDoS UE perspective, this observe-able load balance and congestion activity appear to be the intended outcome from the DDoS attack = DDoS mission accomplished. From the legitimate UE and network perspective, the DDoS UEs are fighting and blocking each other before they are able to reach the DDoS victim = DDoS mission thwarted.

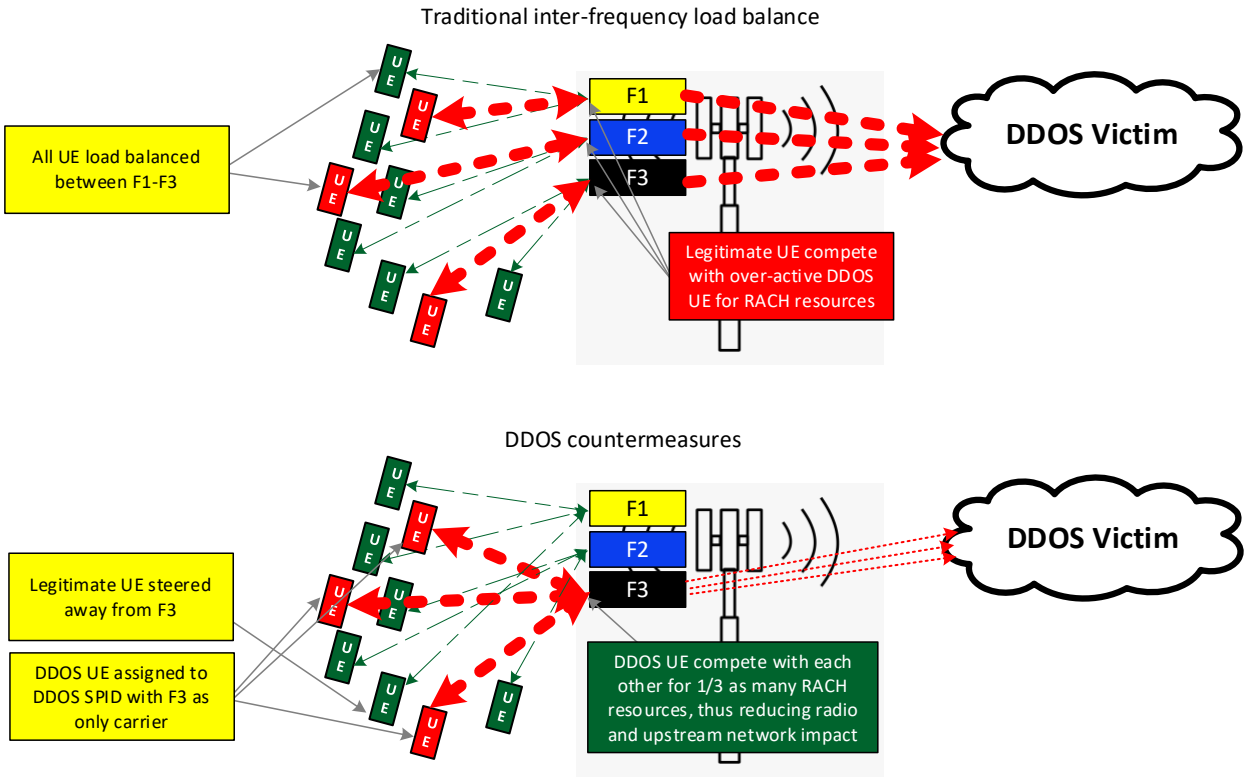

Figure 4-5: Inter-frequency load balance for covert DDoS countermeasures.

In this case, DDoS countermeasure effectiveness increases with the number of DDoS UEs, and the interference and blocking they cause for each other at the leading edge of their attempted transactions.

5 Summary and Next Steps

In the above sections, we have described how radio and blockchain techniques can be combined to form a distributed and powerful IoT DDoS detection, location and covert countermeasure

mechanism. We have explored and shared initial results for the radio DDoS detection component, including approximately 60% DDoS prediction accuracy.

Future research will include exploration of individual and combined Blockchain, radio location and countermeasure components of this proposal.

6 ACKNOWLEDGEMENTS

The views expressed in the IIC Journal of Innovation are the author's views and do not necessarily represent the views of their respective employers nor those of the Industry IoT Consortium®.

- Return to *IIC Journal of Innovation landing page* for more articles and past editions