Wireless Sensor Network for Enabling Private Cloud on board Naval Ships

Muhammad Faheem, B.Engg

Ramu T Srinivasiah, B.Engg

* *Lekha Wireless Solutions Pvt Ltd, India*
* Corresponding Author. Email: faheem@lekhawireless.com

Synopsis

Abstract— A typical warship has thousands of sensors. Sensor input is key for the ability of the ship to float as well as to carry out all practical operations at sea. Live readings of multiple sensors are visualized and processed by personnel at the bridge to take decisions. Digitization of sensor data enable ability to use high end computers for complex analysis of sensor data using Artificial Intelligence algorithms. Storage and monitoring capability of historical sensor data helps predictive and preventive maintenance of all the equipment onboard the ship thereby enhancing safety and operational efficiency. Hierarchical private IOT (Internet of Things) cloud setup on each ship can do wonders in rapid expansion and deployment of IOT applications and data analytics. Important sensor data shall be connected to Private IOT cloud over Internet Protocol (IP). Wireless Local Area Network (LAN) infrastructure reduces the amount of cabling required in ships thereby bringing down the cable density in the ducts and easy maintenance. While the displays at the bridge continue to focus on critical parameters, connected smart phone applications for accessing and visualizing the sensor data improves the comfort level of ship crew to access data and enhance operational efficiency.

This paper focus on choice of 5G NR technology for setting up of machine-to-machine communication infrastructure. 5G NR offers large density of sensor nodes, quality of service parameters and secured communication. How the 5G user end device ecosystem offers low cost and low power wide area network (LPWAN) can be exploited for addressing the sensor network onboard ship. The evolving 5G NR standards has an immense potential to transform sensor network, smarter ways of accessing data and enable AI/ML algorithms for analysing sensor data.

Lekha Wireless is an active member contributing to 5G standards through TSDSI (Telecommunications Standards Development Society, India), a standards development office (SDO) representing India at 3GPP. Lekha has experience of deploying 4G and IOT network for private enterprise and naval requirements.

Keywords: IOT; LTE; 4G; 5G; Wireless; Integration; Marine systems

1. Introduction: Internet of Things

Internet of things (IoT) refers to a collection of interrelated devices connected and used for achieving a set of functionalities. In civilian world, devices which are not connected currently will be connected as part of IoT. It is also redefining the interaction between people and machines. From energy monitoring in a factory to tracking supply chains, IoT optimizes the performance of the equipment and enhances the safety of workers. IoT systems can be more effective in monitoring and coordination of manufacturing, supply chains, transportation systems, healthcare infrastructure, and smart city application, among other sectors and processes.

Figure 1 below shows an exhaustive list of devices and application mapping in the IoT world.

Authors' Biography

Ramu T S is Founder and Director at Lekha Wireless Solutions Pvt Ltd, Bangalore. He has experience of 25 years in wired and wireless communication technology and product development. Lekha Wireless is an Indian technology company developing 4G, 5G technology and special waveforms for Software Defined Radios (SDR) developed for defense and industrial applications. He has experience of leading the teams in developing multiple products starting from idea to prototype, then to production and deployment. At present he is responsible for go to market strategies for the 4G and 5G products to telecom and private network verticals.

Muhammad Faheem is Director Engineering at Lekha Wireless Solutions Pvt Ltd, Bangalore. He has over 22 years of experience in Wireless and multimedia product development. He has worked on Multiple wireless standards such as CDMA, NG-PHS, WiMAX, LTE and NBIOT. He has architected and developed systems on various Multicore and Multi DSP solutions for wireless products. During last 12 years, Faheem has worked specifically on 4G and NBIOT systems.

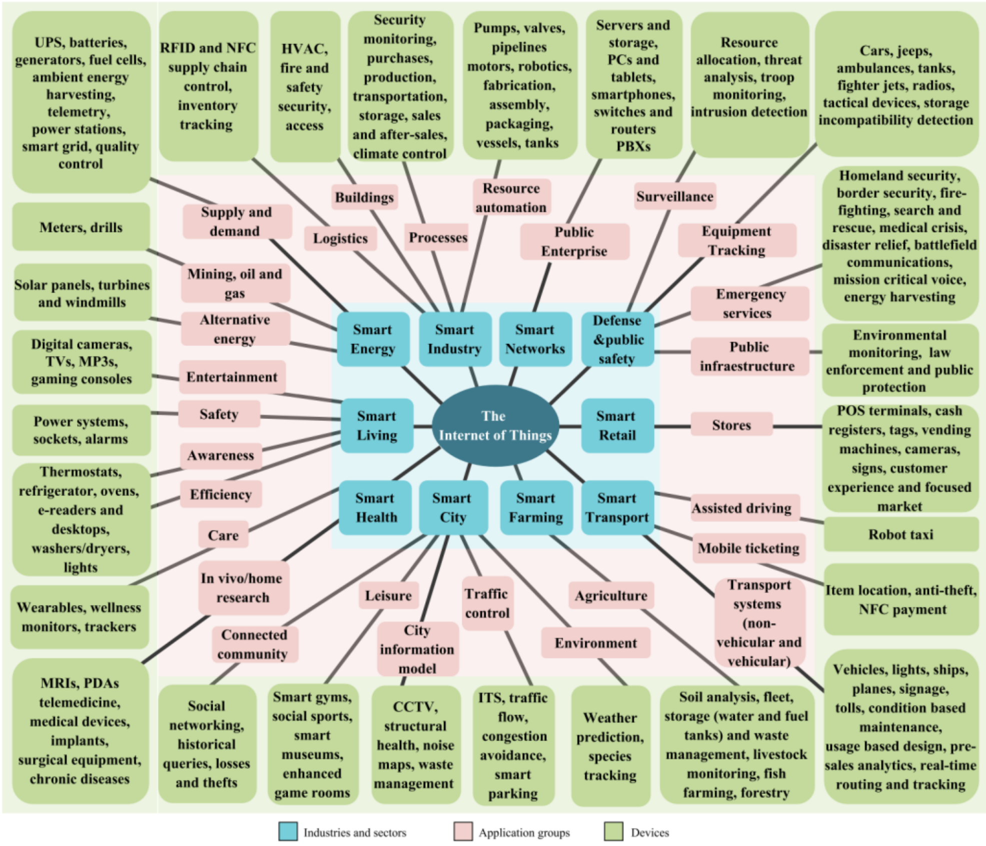

Figure 1: Devices and Application on the Internet of Things (IoT) (Fraga-Lamas et al., 2016, p, 2)

It was defence sector that pioneered the internet which has redefined today's telecommunication network. There are many advances in telecommunication like Internet of Things, big data analytics, cloud computing and Artificial Intelligence that has the potential to transform the next generation connected smart military platforms.

Over the course of the last few decades, Naval forces across the globe have faced a tsunami of challenges in efficient management of ship. The IoT technologies are applied to automate marine-related operations as well as creating novel smart devices. Human to machine interactions and machine to machine communication have become far more critical in case of smart marine operations and ubiquitous network connectivity holds the key. Data centric decision-making process is the critical for more efficient Naval Operations especially in Command-and-Control systems and Platform Management Systems. This paper proposes a wireless communication infrastructure that is based on 3GPP based 5G technology as the infrastructure to enable adoption of many new technologies like AI, cloud computing etc. over the collated data.

1.1. Wireless Connectivity for scalable and efficient IOT

Connectivity is the foundation for IoT, and the type of access required will depend on the nature of the application. Based on available information, wireless IoT is almost non-existent in warships. But it is the only way forward for better efficiency and reduction in watch-keeping and other manpower requirements. Below are major classifications of wireless IoT devices based on radio frequency of operation.

A. Unlicensed Band

Mostly devices operating in unlicensed spectrum enable Short-range connectivity with limited, radiation, QoS and security requirements typically applicable for a home or indoor environment. Unlicensed Low Power Wide Area are new proprietary radio technologies like SIGFOX and LoRa are designed solely for machine-type communication (MTC) applications addressing the ultra-low-end sensor segment, with very limited demands on throughput, reliability or QoS. Technology and standardization effort in unlicensed bands are scattered and newer technologies defined are not compatible with predecessors.

B. Licensed Band

IoT applications that depend on wide-area network (WAN) coverage employs Licensed band. Globally, licensed band networks are run by cellular operators with clear path for evolving current generation to the next generation networks. These cellular technologies are part of an organized sector that primarily targets high-quality mobile voice and data services. Most successful cellular technologies are standardized by 3GPP like GSM(2G), WCDMA(3G), LTE(4G) and 5GNR (5G) that utilizes licensed spectrum for connectivity. While 2nd and 3rd Generation specifically focussed on human-to-human type communication, 4th and 5th Generation included focus for new functionality like human to machine and machine to machine communication. New radio access technology, narrowband IoT (NB-IoT) which is part of 4G and is tailored for emerging low power wide area (LPWA) applications. NB-IoT technology is evolving as massive machine type communication (mMTC) as part of 5GNR.

In civilian application a large share of the IOT devices served short-range unlicensed radio technologies while we strongly believe that for the Internet of Military Things (IoMT) a significant proportion will be enabled by wide area networks (WANs) that operates in licensed band. Marine use cases demand varied coverage needs. These requirements can be majorly classified as

a) Highly localized such as stationary installation creating a hotspot. Generally low power access points are used in closed spaces.
b) Wider area network established to cover significant portion of ship. High power base stations with a high gain antenna mounted on mast on top of the deck are used.
c) Global service coverage. Satellite based communication are commonly used for covering relatively large geographic area globally. Non-Terrestrial Network (NTN) is being standardized as part of 5G NR.

There are many competing technologies that are deployed for IOT networks, rest of the paper elaborates on using IoT network based on 4G and 5G NR standards.

1.2. Wireless IOT Challenges

Even though marine IOT network would demand network to be deployed in much harsh conditions and high degree of security, below cellular IOT challenges are very much relevant for IoMT as well:

- Device cost – clearly a key enabler for high-volume, mass-market applications, enabling many of the use cases. 5G IOT devices are cost effective for the mass market applications.

- Battery life – many IoT devices will be battery-powered, and often the cost of replacing batteries in the field is not viable. 5G IOT devices are enabled with coin sized battery which can have a battery life of 10 years.

- Coverage – Most major combatants such as Destroyers, Frigates and Carriers have close to 13 to 14 decks in all, where deep indoor connectivity is a requirement for many applications in the utility area. 5G IOT has the ability to penetrate deep indoor providing connectivity for many applications in the utility area.

- Scalability – in order to enable a Massive IoT market, networks need to scale efficiently. The initial investment required for supporting a limited number of devices has to be manageable, while on the other hand, the network capacity must be easy to scale to handle thousands – or millions – of devices. 5G IOT network capacity can be easily scaled to handle such dense device scenarios.

- Diversity – connectivity should be able to support diverse requirements from different use cases. One network supporting everything from simple static sensors to tracking services, to applications requiring higher throughput and lower latency is essential in terms of total cost of ownership (TCO). 5G with In-band IOT network can support multiple device type with varied data rate requirements.

2. Narrow Band IoT: Introduction

NB-IOT, is an offshoot or upgrade of the commercial 4G LTE solution and continues to evolve as part of the 5G NR standard. Its unique features of low power consumption, low implementation cost and low complexity makes it attractive to most of the IOT solutions. NB-IoT provides respectable range and bandwidth to realize the requirement of providing IoT devices and connectivity while co existing with wide band 4G and 5G network.

NB-IoT can connect large number of devices, as high as 50,000 per cell. NB-IoT features meet many challenges. NB-IoT can connect many devices to the network and create many new applications both at edge location and central location. It can be optimized for applications that need a small amount of data for a long period of time. NB-IOT supports power-saving mode which enables battery operated end points with long life as high as 10 years without battery replacements.

These are the basic technical details of the network architecture of NB-IoT.

- **NB-IoT Basic Technical Features**: The extended coverage of NB-IoT is 20 dB better than GPRS. The extended coverage of NB-IoT is 164 dB MCL (Maximum coupling loss). GPRS has a 3% outage for the indoor area with 20 dB penetration loss because of the low MCL of 144 dB. There is a different range for the different network for connecting the devices. We can connect about 40 devices per household with NB-IoT.

2.1. System Architecture

As shown in the diagram below a 5G IOT Network involves User Equipment / IOT devices connecting to Infrastructure. 5G Infrastructure consists of Radio Network (RN), Packet or Core network (CN) and Network Applications. CN aggregates data from multiple RN to network application at edge. There are interfaces defined where multiple CN can interconnect to enable a secured centralized or private cloud within ship. Figure 2 below illustrates the 5G IoT network architecture.

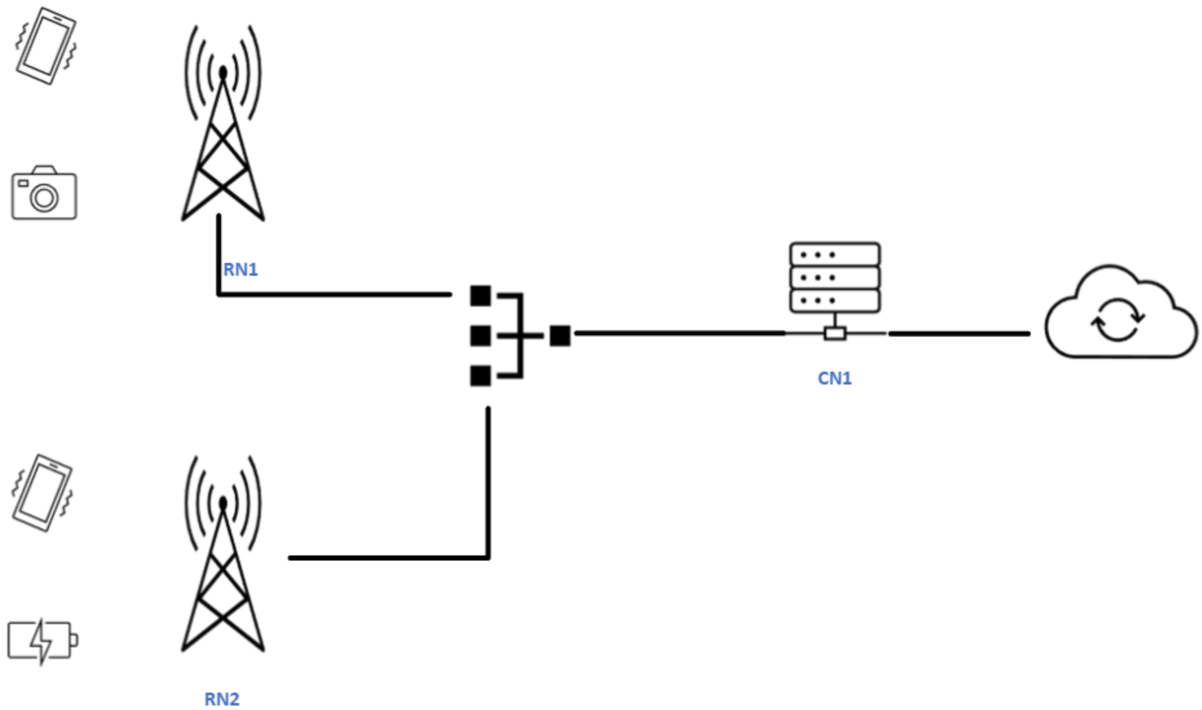

Figure 2: 5G IOT Network Architecture

2.2. Deployment Modes

NB-IOT network can be deployed in Standalone mode or Non-Standalone mode. Figure 3 shows the pictorial representation of the modes and further details on the modes are discussed further.

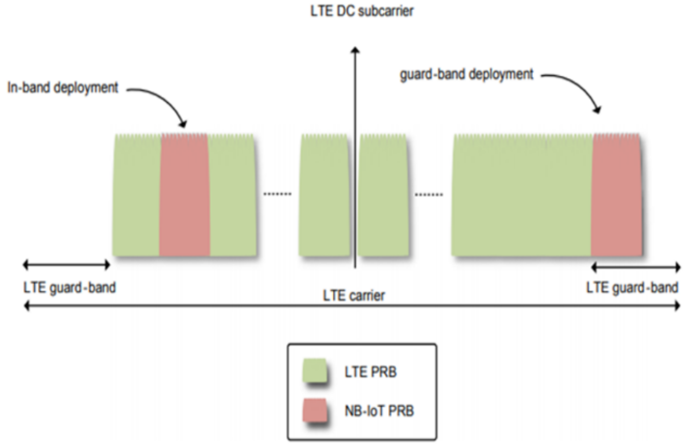

Figure 3: NB-IOT Deployment Modes (Olof et al., 2019, p, 224)

a) Non-Standalone mode.
In non-standalone mode the IOT network co-exists with a typical 4G and 5G wide band network. 5G Radio Network can operate from frequency Bandwidth raging from 5MHz up to 100MHz. Here one or more channels of 180 KHz bandwidths are reserved for IOT connectivity. As shown in the Figure 3 the reserved channel for IOT can be allocated at either edge of 5G band referred as "guard-band deployment" or inserted anywhere in the middle also called "In-band deployment".

Generally, in this deployment configuration the network enables all type of communications like human to human, machine to human and machine to machine.

b) Standalone mode
In standalone mode an independent access point or a low power base station provides coverage to the end IOT device over a narrow channel of 180 KHz bandwidth. Standalone mode is suitable for low bit rate machine to machine type communication like connecting the sensor nodes to a server. Standalone deployments are preferred for providing connectivity in the closed space deep inside and across the decks of ship.

2.3. Security Architecture

Following diagram indicates the entities requires as part of NB-IOT network architecture and detailed on each of the entities further.

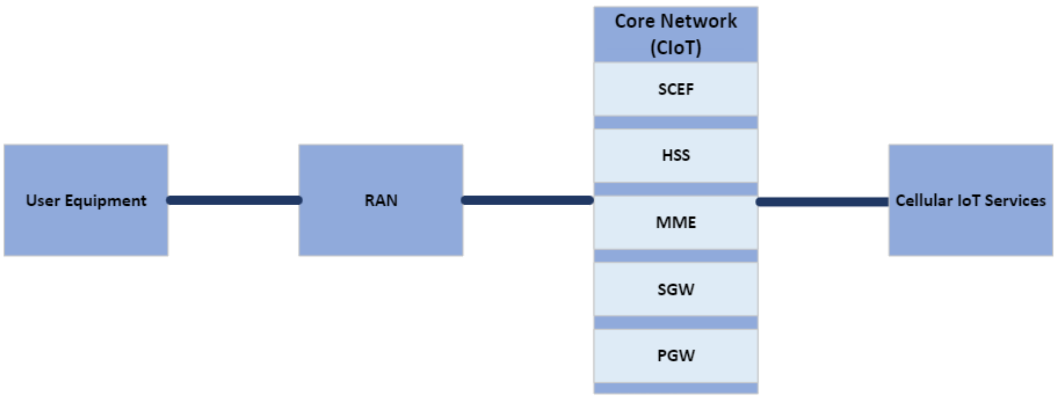

Figure 4 NB-IOT Network Architecture (GSM Association, 2017, p, 9)

Figure 4 shows the network architecture with Core Network blocks detailed for cellular IoT. Following blocks are contained within Core Network:

- SCEF: Service capability Exposure Function.
- PGW: Packet Data Node Gateway.
- S-GW: Serving Gateway.
- HSS: Home Subscriber Server.
- MME: Mobility Management Entity.

MME – Mobility Management Entity: The mobility management entity is playing an important role in Core Network architecture. The mobility management entity is the main signalling node in the Core Network. The main function of the serving gateway is the routing and forwarding of user data packets. Also, it is responsible for providing mobility between 5G and other networks. The PGW is responsible for interfacing between the 5G network and other packet data networks.

HSS: Home Subscriber Server: The function of HSS is to communicate with the network and provide subscriber profiles and authentication info. The database stores info of the subscriber and helps in authorization and details of the device. To establish a secure connection between an end device and the NB-IoT network, both parties must authenticate to each other. For this purpose, the USIM contains a unique identification number that includes the IMSI as well as a 128-bit long master key K. The HSS stores every valid SIM, its master key K and its authorizations. For mutual authentication, the end device and HSS prove that they possess the master key. However, to be precise, it is the USIM – not the device or the user – that authenticates itself towards the network. Snow3G and AES128 are considered as encryption algorithms in NB-IOT. eSIM can also be used for USIM in NB-IOT.

The **SCEF** is a product deployed in a policy management network that interacts with the internet of things devices as a machine-to-machine communication. This module takes care of non-IP traffic.

3. Networking in Naval Ships

As shown in Figure 5, it is a common sight to observe large bundles of ethernet cables connecting various parts of the naval ships. The sensor data network is one of the major contributions to the wiring requirements including switches and routers. Any introduction of connected sensors during the life of ships would require complete re-wiring to the control station. This paper proposes an alternate mechanism that should be considered in the ship building through which a sensor network is built and the introduction of advanced sensors post ship building would be seamless. To achieve this transition, numerous applications need to be developed to make them smart. As an important step towards this we are considering a use case where proposed IoT-based network enables wireless connectivity to establish sensor network onboard ship.

Figure 5: Typical Cable Tray

3.1. Sensor Network

The concept of Sensor Network on board ship is discussed in this section. These sensor data are wireless connected and displayed on the display panels of the flying bridge over NB-IOT network. This solution can be quickly deployed in any location on board the ship by deploying multiple NB-IOT eNodeB across the ship. Wireless connectivity thus established enables next generation cost-effective sensors with ease of maintenance during the life of the ship.

Extensive use of IoT devices in defence networks will become inevitable. Also, there is a rise in the number of use cases that demands broadband connection, necessitating large deployments. Entire defence network for various military scenarios including the requirement of network onboard a Naval Ship can be categorized as below types:

- Communication between personnel to personnel – This involves voice and Video calls and exchange of messages or chatting.
- Machine to Machine communication –Include industrial instrumentation, enabling a sensor or meter to communicate the information it records to an application that can use it for further processing.

Platform Management and Command and Control systems are treated logically as different data streams with appropriate Quality of Service requirement such as priority, bandwidth and latency etc.

3.2. 5G Network in Naval Ship

The potential applications for the IoT run into the millions, with a huge variety of requirements regarding cost, battery life, coverage, connectivity performance (throughput and capacity), security and reliability. Some devices will only send a few messages per day – such as status indicators for temperature – while others may need to transmit a video stream from a combat operation, for example. The difference in throughput requirements is huge. As the services within Naval ships need to handle several applications, it may be of great benefit to be able to harmonize communication modules, so that they all use the same underlying radio solution to reduce operational and fault management effort and complexity. In this case we would need to deploy the system with 5G and NB-IOT in order to cater to the wide variety of the applications where In-band solution should be considered.

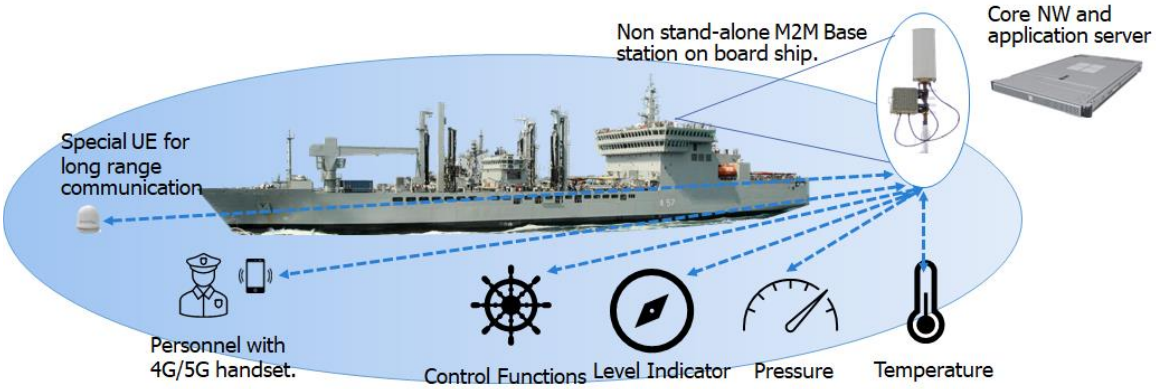

Figure 6: Proposed 5G Naval Network Deployment

Figure 6 shows the typical deployment scenario for a 5G IoMT Network on board Naval ship. With this network connectivity of all the low data rate equipment connected to sensors are done via NB-IOT network and medium and high data equipment are connected through 5G Wide Area Network.

3.3. Coherent Distributed Architecture

It is important to consider the network within the ship to be coherent with the Naval Architecture. Network deployment needs to consider the inherent coverage issues that would come into picture within multiple decks of the ships. NB-IOT having good coverage helps in this case. Having said that one should still consider deploying multiple NB-IOT base stations to cover the dark spots within the ship and a 5G base station to communicate within and outside the ship. To be coherent with the ship design with multiple compartments of the ship should be covered via different Network in a Box (NIB) entities, which contains Radio Network, Core Network and Application server within single box. This enables Edge Computing for a group of sensors within each compartment. Multiple NIBs and Core Networks within the ship are connected to the application server and in turn to the dashboard. 5G Wide Area Network also uses USIM module for authentication.

Every NB-IOT as well as 5G base stations would be connected to one or more Core Networks which in turn is connected to one or more application cloud servers hosted within the ship. This distributed network takes care of high availability and redundancy within the ship for any scenario where an attack affects to certain parts of the ship. This architecture enables various IoT as well as high data rate applications to be run using the network. Possible applications that can be run with the system is discussed in Section 4.1

The strength of cellular technology Is the expertise in managing multiple networks, It is also a primary requirement as far as warships are concerned. Typical network architecture that is proposed in this paper is shown below in

Figure 7. Multiple small cells should be deployed in order to make sure the coverage is adequate in all parts and floors of the ship.

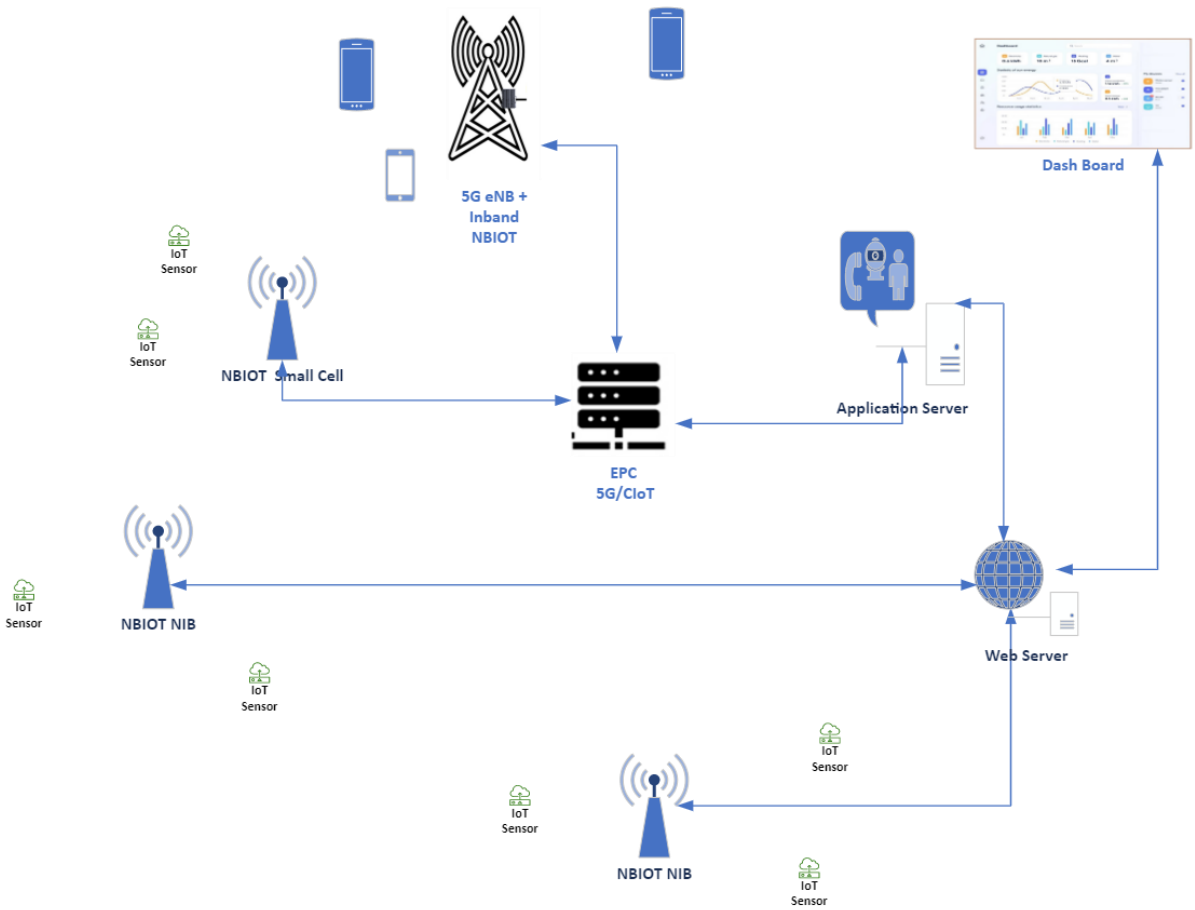

Figure 7: Proposed Distributed Network Architecture

3.4. Broadband Network Advantage

Voice and video communication within and outside ship is possible with Broadband network. Figure 8 indicates the scenarios for the usage of 5G Enhanced Mobile Broadband (eMBB) network for ship to ship and ship to boat communication with broadband applications. It can provide a range up to 100KMs. This will enable Ship to shore communication as well with the right deployment scenarios.

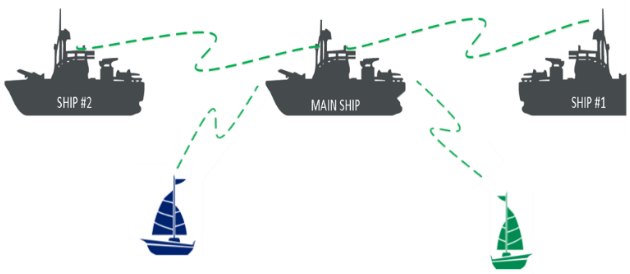

Figure 8: Inter ship Communication Scenario

Application for Broadband network also include ship to shore communication which greatly enhance in the Drydock Maintenance.

4. Application Design

With network deployment scenarios discussed in the previous section, the usage of the network would be complete with appropriate application design in place. Sensors would be sending data at a very long interval. The design of the system should take care of various sensors and appropriate application for each of the sensors. The data from all the sensors should be brought to a Dashboard with the details designed for ease of use as it needs to deal with thousands of sensors possibly. The application should also have provisions to prompt the user in case with warnings and alarms as appropriate. These can be through phones and tabs over 5G network. It should also have provision for different user group for accessing information from different NIB / group of sensor information. Captain of the ship will have access to the master Dashboard for all the information across groups. Hence the application design essentially should consider, but not limited to, the following frameworks as part of the platform:

- Software Framework
- Cloud Framework
- Mobile Application
- Dashboard Framework
- Security Framework

All the application servers should be hosted within the ships to avoid any delays connecting to internet cloud with any other mechanism. This should also consider high level of security in access at various levels.

Examples of dashboard captured below in Figure 9. Such dashboard can be used for onboard or at the dock when the ship is approaching. This picture is indicative only.

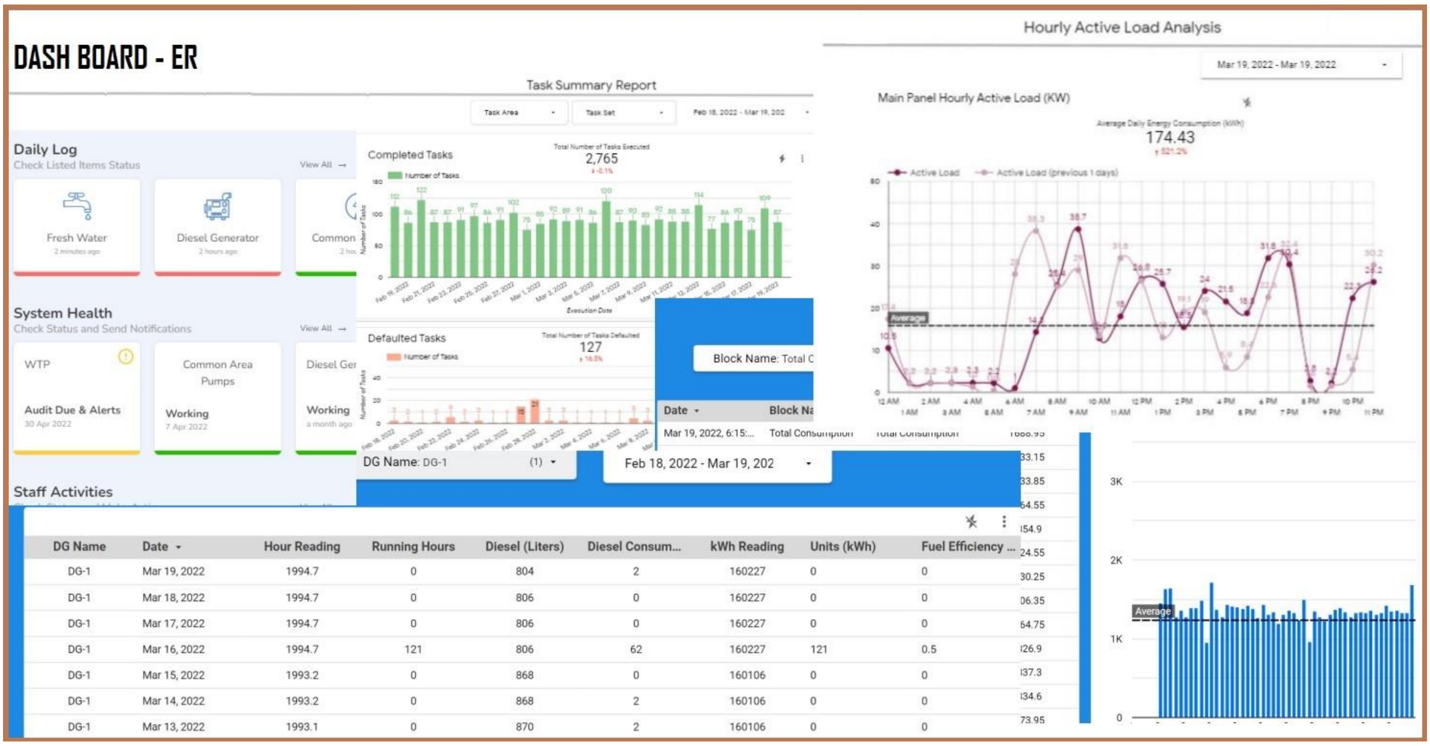

Figure 9: Indicative Typical Dashboard Example for Engine Room

4.1. Proposed Applications

Until now, the deployment of IoT-related technologies for defense and public safety has been essentially focused on applications for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) (www.defenseone.com), and fire-control systems. This is driven by a predominant view that sensors serve foremost as tools to gather and share data and create a more effective Command and Control (C2) of assets. IoT technologies have also been adopted in some applications for logistics and training, but their deployment is limited and poorly integrated with other systems. Besides, IoT functionalities are useful for establishing advanced situational awareness in the area of operations. Commanders make decisions based on real-time analysis generated by integrating Sensor data from unmanned sensors and reports from the field. These commanders benefit from a wide range of information supplied by sensors and cameras mounted on the ship as well as VBSS Team, and manned or unmanned boats. These devices examine the mission landscape and feed data to other ships which are part of the fleet for taking necessary actions. Some of the data may be relayed to a Command Centre where it is integrated with data from other sources.
Defence applications that can be considered for IoT integrations are listed below: -

(a) **Internet of Military Things (IoMT) Dashboard for C4ISR**: A military commander can have access to a comprehensive dashboard which has data as well as output of AI / ML algorithms taking input from various sensors and cameras. This provides situational awareness and real time data helping in controlled and coordinated operations.

(b) **Intelligent Fire Fighting System**: IoT enabled Fire Fighting Systems can improve performance of the system increasing the efficiency with minimal human intervention. It can have lever status, various release systems, firefighting bags status and location and contents of the same, extinguisher / equipment status and location, leakages at Engine Room etc are few parameters that can be considered to bring to dashboard

(c) **Storm Preparation and Handling**: There are various parameters to be checked in cases where there is expectation of storm, and this involves checking various parameters from sensors which can be brought to Dashboard via IoT. Couple of parameters that can be considered is Anemometer, Barometer etc.

(d) **Energy Management**: Energy management can be brought to the dashboard to indicate whether the energy generation is happening or utilization from the shaft. Various generator status such as Turbine Generator, Diesel Generator and Generator Motor Information from the Engine Room (ER) can also be brought to the Dashboard which can be associated with the AI for various analysis.

(e) **Military Logistics with Combat Management System (CMS)**: Solution for equipment and ammunitions can be considered here with each equipment and ammunition having ID / Tag. ID and location can be tracked from shore to on board and information of the these especially as weapons will always be useful for the commander.

(f) **Connected Sailors**: Wearables with integrated Camera and mic provides better efficiency for the sailors to execute the operation with increased situation awareness. Wearables can also share health parameters of the Marines to the Health Management System which can run AI to warn Marines and commander to take precautions. Connectivity with other boats within few nautical miles also can be achieved with the 5G network on board for eMBB.

(g) **Guided Weapons**: Connected weapons can be a use case which can utilize the network on board.

(h) **Disaster Management**: Network on board has immense opportunity in operations such as disaster management operations with Drones and Robots. This can greatly reduce possibility of injury and fatality with increased safety and security.

(i) **Dry Dock and Maintenance**: Data available from various sensors are transferred to the maintenance applications at the service yard. The data available also can be used for predictive and reactive maintenance at the Dock which can utilize the AI application output.

(j) **Autonomous vehicles**: Unmanned or even autonomous Underwater, surface (boats) or aerial vehicles launched from ship can be controlled and the data can be accessed and managed using the network.

5. Network Deployment Experience on Naval Ship

As part of a program called iDEX (Innovations for Defence Excellence) (www.idex.gov.in)from Ministry of Defence to setup 4G network over naval ship, naval trials were executed. The company developed its 4G product for typical cellular network. When Indian Navy wanted to adopt the 4G technology, they had specific custom requirements both in terms of hardware and software which was prerequisite for conducting field trails at Sea. Following features were part of the trial and here we discuss how the challenges faced were resolved.

a) Radio coverage range was way higher than typical cellular network:
   - 4G system supports large preamble formats for extended range scenarios, which is seldom used in a commercial network. With these preamble formats and high-power radios. Additionally high power UEs were also used to extend the coverage to connect to the ships which are several nautical miles apart.

b) Navy wanted voice, video conferencing messaging etc without need of connectivity to internet.
   - Video conferencing application server was integrated to NIB module to make sure the cloud applications are hosted locally to work without internet connectivity.

c) Given the network is installed on a moving platform there were specific innovations brought in to track BTS and user locations using IRNSS (Indian equivalent of GPS).

As part of the mission, a team of engineers sailed along with Indian Navy to demonstrate the network. Through this interaction, team could collate more requirements that could help the operations. Constant engagement with navy team, learning and evolving the product is key for defence projects. Indian Navy highly appreciated and valued company's co-operation which helped them to get acquainted with the technology and plan the operations more effectively.

This experience helped to bring out the network architecture for this paper with better understanding of the scenarios and challenges within the ship for wireless connectivity.

6. Conclusion and Future Work

IoMT can revolutionize the way marine management is handled and drastically reduce the human to machine interfaces in various avenues. This can also increase the manpower efficiency in the ships. This will also change the way wars are fought.

Operational efficiency is greatly improved with such a system in place. Availability of a system with NB-IOT and 5G network within a ship will greatly help in IoMT. This would also enable Ship to Ship and Ship to Boat communication in various scenarios. The inherent support of high encryption within standard for data security enables the proposed system as an obvious choice of 5G.

The selection of 3GPP standard for networking also enables future evolutions, as system can be upgraded over the life span of the ship. Wireless broadband connectivity also plays a role while the ship is at the dock for maintenance which enables maintenance preparations miles before the ship approaches the yard.

Hence the advantages and applications discussed in this paper strongly suggest the Naval Architecture to consider 5G network to be an integral part of Ship Building with following considerations:

- **Radio Planning** should be considered for determining number and type of radios to cover length and breadth of the ship.
- **Scalable system on board** ship to enable addition of new sensors / radios, new applications etc. over the lifetime of the ship.
- **EMI/EMC Consideration**: Ships, especially warships operate in a very dense Electro-magnetic environment. Proposed 5G system should coexist with other systems.
- **Redundancy**: Distributed network architecture with coverage overlaps to ensure High Availability of network.

Non-Terrestrial Network (NTN) connectivity is also being added to 5G standards which will be a big boost to the navy ships to connect to the command headquarters with the help of defense satellites enabling the use of 5G handsets across Navy ships. Future work will focus on adding NTN aspects to the proposed architecture.

Acronyms

3GPP	Third Generation Partnership Project
4G	4th generation; see LTE
5G	5th generation systems under 3GPP
5G NR	5G New Radio
AES	Advanced Encryption Standard
AI / ML	Artificial Intelligence / Machine Learning
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CN	Core Network
GPRS	General Packet Radio Service – 2nd Generation Standard
GSM	Global Standard for Mobile – 2nd Generation Standard
eMBB	Enhanced Mobile Broadband
EMI / EMC	Electromagnetic Interference / Electromagnetic Compatibility
eNodeB	Evolved Node B – Base station network element in LTE
eSIM	embedded-SIM
HSS	Home Subscriber Server
iDEX	Innovations for Defence Excellence
IoMT	Internet of Military Things
IOT	Internet of Things
IP	Internet Protocol
LAN	Local Area Network

LoRa	Long Range Radio
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution
MCL	Maximum Coupling Loss
MME	Mobility Management Entity
mMTC	Massive MTC
MTC	Machine-Type Communication
NB-IOT	Narrow Band IOT
NIB	Network In a Box
NTN	Non-Terrestrial Network
PGW	Packet Data Node Gateway
QoS	Quality of Service
RN	Radio Network
SCEF	Service capability Exposure Function
SDO	Standards Development Office
SGW	Serving Gateway
SIM	Subscriber Identity Module
TCO	Total Cost of Ownership
TSDSI	Telecommunications Standards Development Society, India
USIM	User Services Identity Module
VBSS	Visit, Board, Search, and Seizure – Maritime actions
WAN	Wide Area Network
WCDMA	Wideband Code Division Multiple Access – 3rd Generation Standard

References

C4ISR: The Military's Nervous System https://www.defenseone.com/insights/cards/c4isr-military-nervous-system/ (Accessed on 12-July-2022)

Fraga-Lamas, Paula & Fernández-Caramés, Tiago & Suárez-Albela, Manuel & Castedo, Luis & González López, Miguel. (2016). A Review on Internet of Things for Defense and Public Safety. Sensors. 16. 1644. 10.3390/s16101644

GSM Association, 2017, NB-IoT Deployment Guide to Basic Feature set Requirements, Official Document CLP.28

Innovation for Defence Excellence https://idex.gov.in/ (Accessed on 19-September-2022)

Olof Liberg, Marten Sundberg, Eric Wang, Johan Bergman, Joachim Sachs. (2019) Cellular Internet of Things Technologies, Standards, and Performance Edition. E-book [pdf] (Accessed: 22 July 2022)

Bibliography

1. Ericsson Mobility Report, November 2015, http://www.ericsson. com/res/docs/2015/mobility-report/ericsson-mobility-report-nov-2015.pdf
2. https://www.sharetechnote.com/html/Handbook_LTE_NetworkArchitecture.html
3. https://www.sharetechnote.com/html/Handbook_LTE_NB_LTE.html
4. https://www.sharetechnote.com/html/5G/Handbook_5G_Index.html