Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 171 (2020) 2665–2674

Procedia Computer Science

www.elsevier.com/locate/procedia

Third International Conference on Computing and Network Communications (CoCoNet'19)

5G for Military Communications

Anshu Bhardwaj*

CAIR DRDO Bangalore, India

Abstract

5G networks are in advanced stages of trials across the globe and the deployment will begin as early as 2020. In this survey paper, the possible use cases of 5G networks in the military context is captured. After the introduction, the various key 5G technologies – mmWave, massive MIMO, HetNets, SDN, NFV, D2D Communication and the challenges in road to 5G are briefly discussed. The paper then focusses on security challenges and services as offered by the 3rd Generation Partnership Project (3GPP (5G)) Security Association 3 (SA3) group. Future battle space scenarios leveraging 5G technologies are covered next. Finally, the paper touches upon the present status of 5G deployment across the globe with special mention of 5G development efforts by the Government of India, the challenges and the opportunities ahead.

Peer-review under responsibility of the scientific committee of the Third International Conference on Computing and Network Communications (CoCoNet'19).

Keywords: 5G Technology; Military Communication; Security Challenges; Future Battlespace; 5G Roadmap

1. Introduction

Cellular Communications until now was mostly focused on human communications – connect people to people. But the next generation mobile networks (NGMN) (read Fifth Generation/5G) are designed to connect more and more devices to each other. The vision of smart things, smart cities or smart military bases, requires realization of Internet

* Corresponding author. Tel.: +91-80-25244288; fax: +91-80-25342644
E-mail address: anshu@cair.drdo.in

Peer-review under responsibility of the scientific committee of the Third International Conference on Computing and Network Communications (CoCoNet'19).
10.1016/j.procs.2020.04.289

of Things (IoT), where every object will have inbuilt sensors and intelligence to sense and make decisions along with the ability to communicate to every other object, in vicinity that too in real-time resulting in a collaborative environment to meet certain objective, and all this will happen without human intervention. 5G networks are seen as the potential essential infrastructure necessary to make this a reality [3]. 5G will support heterogeneous networks to serve both traditional voice, video and data services in addition to new services that will be enabled by the networked Device to Device (D2D) communication at ultra-low latency in an extremely dense environment (1000x more connected devices than in 4G networks) and with very high reliability.

The above vision of 5G technologies draws a similarity with the operational requirements of military communications of provisioning for interoperable voice, video and data services across a global environment. The capability of 5G technologies to connect sensors with autonomous vehicles and machines with in-built sophisticated artificial intelligence algorithms will mean faster, deadlier, less human warfare [33]. 5G will work on millimetre-wave band, with directional antenna and beamforming techniques (to counter for large-signal attenuations encountered due to smaller wavelength), shared spectrum access (enabled by directivity and low ranges) and provide super high-speed full-duplex communications. These are some of the technologies going to become common among commercial and military communications [33]. Further, since 5G communication will make the machine to machine communications possible without requiring satellites or communication relay aircraft; it will become a keystone of future military technology.

This paper is divided into 6 sections; the first section is an introduction in which capabilities of 5G networks and similarities with military operational requirements are briefly discussed. The second section covers the features, applications and key 5G technologies. In the third section challenges of 5G are presented with a focus on security requirements, challenges and solutions given by various authors as well as 3GPP (5G) standardization body. In the fourth section, applications of 5G for military networks and some of the future battlespace scenarios leveraging 5G technology are presented. The fifth section covers the present status of 5G deployment and roadmap across the globe and the last section is the conclusion.

2. 5G Definition, Goals and Applications

3GPP is the global standardization body for mobile communication that comes up with a new generation of mobile standards, with new capabilities and application areas, almost every decade since the 1980s. 1G was analog but truly mobile-first generation voice-centric network fielded in 1980s. 2G was the first digital mobile communication network that was voice-centric with limited data capabilities launched in the early 1990s. 3G was the first wireless mobile data communication technology that enabled data streaming and mobile internet access, in 2003. 4G was the first all IP wireless data communication technology launched in 2008. The data communication feature enabled by packet switching and almost ubiquitous adaptation of IP protocols in 3G and 4G networks has led to the proliferation of plethora of applications like streaming, eCommerce, social networks, games etc on mobile devices. As the generational change in mobile wireless technology, 5G is expected to be an enabler to a series of services with massive Machine-Type Communication (MTC) like D2D (Device to Device) and Vehicle to Vehicle (V2V) or Vehicle to Infrastructure (V2I) communications, that will minimize the boundary between the digital world and the physical world thereby impacting every aspect of our lives [5].

Experts have identified eight advanced distinguishing features/goals of 5G Systems in [1], [2] which includes throughput ranging from 1Gbps up to 20Gbps; latency better than 1 msec; massive connectivity at super high speed; 1000s of interconnected devices and 1000x BW per unit area; 100% coverage with 99.999% availability; high energy efficiency - 90% reduction in energy and up to 10-year battery life for machine-type communications

The various applications of 5G can be broadly classified into three domains - enhanced Mobile Broadband (eMBB), Massive Machine-Type Communications (MTC) and Ultra-Reliable Low Latency Connections (URLLC). At least 10 fold increase in browsing speeds is the first and foremost requirements in the natural evolution of 4G/LTE to 5G. The target browsing speeds for eMBB platforms will be starting from 1 Gbps with downloads better than 200 Mbps. Interconnected everyday smart devices, vehicles and industrial equipment to realize the dream of IoT necessitates the development of massive MTC. The third instrumental application is URLLC for “mission-critical” applications for real-time data collation necessary for situational awareness and quick decision making.

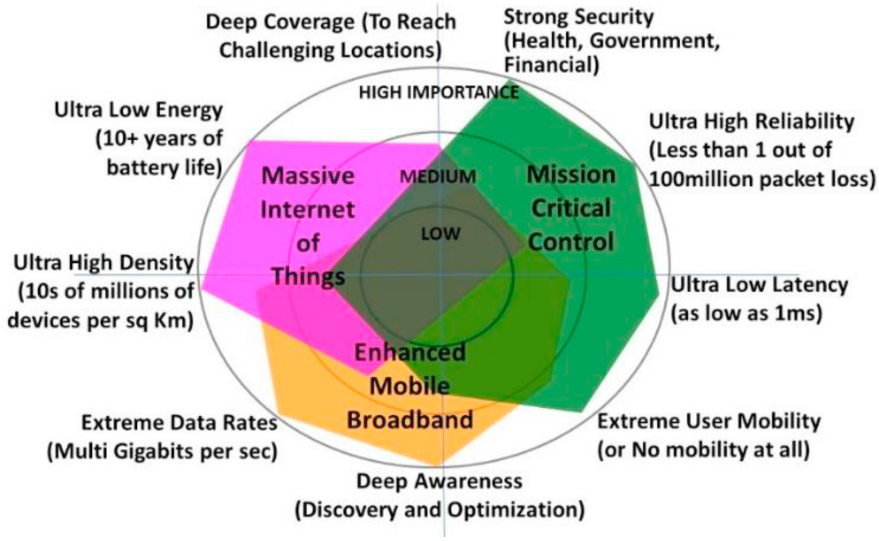

Fig. 1. 5G Applications and Requirements [3,4]

Figure 1 captures the relationship between the target applications and the key distinguishing features for 5G. For Eg. ultra-low energy and ultra-high density is the most important feature required for IoT applications, eMBB applications are necessitated by highly populated and demanding urban population and would be achieved with extreme data rates and as expected for mission-critical applications ultra-high reliability, ultra-low latency and strong security precede all other requirements).

2.1 Key Technologies of 5G

The various new technologies [5, 6] are applied to 5G systems, to meet the above goals are:

i. *Heterogeneous Networks (HetNet)* – Various nodes will have different radio access technologies (RATs) like High-Speed Packet Access (HSPA), Long Term Evolution (LTE), Wi-Fi. This will enable forming of a multi-tier network with each tier having different characteristics such as transmission power and coverage area. With HetNet, it is possible to realize hyper-dense small cells that will address the 1000x capacity challenge. HetNet can be realized by either overlaying a cellular system with small cells of the same technology, that is, with micro, pico, or femtocells; or overlaying with small cells of different technologies (like cellular for macro-cell to cover larger area and wi-fi for femtocell for a single house). HetNet shall achieve significantly better area spectral efficiency (b/s/Hz/m^2) [5].

ii. *Massive Multiple-Input Multiple-Output (MIMO)* - This technology uses multiple co-located antennas (up to a few hundred) to simultaneously serve / spatially multiplex a number of users in the same time-frequency resource. As the aperture of the array grows with many antennas, the resolution of the array also increases. This effectively concentrates the transmitted power towards intended receivers, thus the transmit power can be made arbitrarily small, resulting in significant reductions in intra and inter-cell interference and significantly improve the throughput and Energy Efficiency (EE) performance [6].

iii. *Millimeter-wave (mmWave)*- In the mmWave band, ultra-broadband wireless pipes can be provided due to the availability of spectrum in abundance at present. Also, the small antenna sizes ($\lambda/2$) and their small separations (also around $\lambda/2$), will enable packing tens of antenna elements in just one square centimetre. This, in turn, will allow achieving very high beamforming gains in relatively small areas, which can be implemented at both the Base Station (BS) and the User Equipment (UE) which can further improve the system capacity [5]. However, on the flip side, the path loss is relatively higher at these bands, compared to the conventional sub-3GHz bands; the penetration loss through the buildings is substantially higher at these bands, blocking the outdoor RATs for the indoor users and finally, due to the propagation in Line of Sight (LOS) direction, the radio links are vulnerable to being blocked by moving objects or people. In spite of these limitations, mmWave is being perceived as the most promising spectrum for future networks due to support for massive MIMO and availability of abundant spectrum in this frequency band.

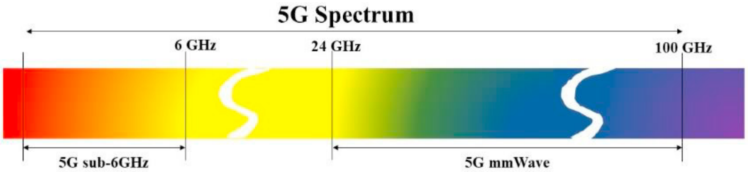

Fig.2. 5G Spectrum [7]

iv. Device to Device (D2D) communications - D2D communications not only enables efficient spectrum usage in 5G but also can effectively offload traffic from Base Stations (BSs). The first challenge in this is the number of devices that need to be connected is tremendously large (50 billion devices need to be connected in the future networked society). The other challenge is for real-time and remote control of mobile devices (such as vehicles) through the network requires an extremely low latency of less than a millisecond. "Tactile Internet" [8], that is targeting a 20x latency improvement from 4G to 5G could be a possible solution.

v. Software-defined network (SDN) - SDN can provide three key attributes, namely logically centralized intelligence, programmability, and abstraction so that scalability and flexibility of the network can be greatly improved and cost can be significantly reduced. SDN suggests decoupling the network control plane from the data plane making higher user plane capacity independent of (relatively low bit rate) control plane resources. Further, different networking mechanisms (i.e. routing, forwarding, access control) are configurable by the centralized Controller in the network, supporting dynamic network topology readjustments and reconfiguration for different networking mechanisms. Also due to the programmable centralized controller, easy and quick adaptation of the infrastructure to novel networking mechanisms such as Cloud Computing, the Internet of Things and others will become possible[6].

vi. Network Functions Virtualization (NFV) and Networking Slicing- NFV actually allows the provisioning of virtualized networking functions in the network edge, sharing aspects of Network as a Service (NaaS). As such, virtualization techniques allow the implementation of network functions in software able to run independently of the underlying server hardware [1]. The core hardware provided by the operator can be virtualized into a logical structure, both in terms of network and processing, into which different services and functions can be virtualized. In this way, actual network operation entities can be virtualized in a multi-version and multi-tenancy way, allowing services and functions to be rapidly scaled as required while reducing maturation and Time to Market with Capital Expenditure (Capex) reductions [5]. As a result, barriers associated with proprietary hardware are overcome, greatly simplifying the deployment of novel networking services. Network slicing is the ability of the network to (automatically) configure and run multiple logical networks as virtually independent business operations on a common physical infrastructure. Network slicing is already being used in a few Enterprise cases but will become a fundamental architecture component of the 5G network.

3. Challenges in 5G Deployment

The Biggest Challenge in 5G is due to a very large number of interconnected devices, including critical infrastructure, with asymmetric resources (size computational resources, power requirements, BW etc) to be used in a completely new paradigm of IoT. To ascertain desired functionality the challenge is security of radio interfaces, security of devices, security of networks, protecting against Denial of Service (DoS) attacks on the infrastructure; Distributed control systems requiring coordination to prevent Signaling storms; preventing DoS attacks on end-user devices (operating systems, applications and configuration data on user devices) and so on. These challenges are also highlighted by Next Generation Mobile Networks (NGMN) and highly discussed in the literature[1]. Massive connectivity will increase the attack surface manifolds for the 5G network. Also, the impact of attack will be seen more deeply because of the challenges in the containment of a successful attack, due to transient boundaries inter and intra-network arising out of logical separation (by NFV and SDN) of the underlying networking and processing infrastructure rather than physical separation.

3.1 Security Challenges and Possible Solutions for 5G

Security has been always a major concern for wireless communications and with IP becoming the backbone of cellular communication now, all threats to an IP network becomes inherent to cellular networks. With each generation of mobile telephony – 2G to 3G to 4G/LTE, security mechanisms have evolved and added more robustness compared to its predecessor generation. For example, mutual authentication was introduced in 3G as a step forward to only client authentication by the network in 2G networks. This enabled devices also to authenticate the network to protect attacks from rogue Base Stations. With increase in computing resources, stronger crypto algorithms with larger key lengths have been introduced in 4G along with a forward key separation in handovers for more secure mobility management. With smartphones being used for practically any application now, more effective privacy protection is considered important in LTE. The vision of 5G is to serve service verticals and not just provide high throughput to humans [9]. 5G is envisaged to connect critical infrastructure like the power grid, public transport, medical database, autonomous vehicles etc. The catastrophic impact on the society due to any security breach at the network level, device level or at data level that would adversely affect the decision making, is the worst nightmare for security systems as well as network and device designers. A number of security threats and solutions have been presented by various authors [1,2,9,10,15] - classifying in terms of generic security requirements, applications perspective or technology perspective. In this paper, the various threats are broadly classified under three categories- threats due to wireless nature of the network, threats due to vast deployment of end devices of diverse natures and threats on infrastructure components like servers, base stations etc.

The threats to networks can be classified into four categories eavesdropping and Traffic Analysis, jamming, Denial of Service (DoS) or Distributed Denial of Service (DDoS) and Man in the Middle Attack (MiTM) [1]. Eavesdropping and traffic analysis are passive attacks used by an unauthorised receiver without disturbing the ongoing communication and hence it's difficult to detect. An eavesdropper tries to extract information by tapping into the channel and traffic patterns are used to identify the location and identity of the communicating parties during traffic analysis. Jamming is done to disrupt radio signals by the adversary by the intentional generation of interference signals and is an active attack. DoS and DDoS are also active attacks on the network - the radio resources or signalling plane– could be attacked by the adversary. In the MiTM attack, an adversary can intercept, modify and insert messages in the network. Rogue base stations were implanted in the legacy cellular networks to force users to establish connections and enable MiTM attack. As discussed in section 2.1, 5G will have Hetnets where all type of wireless Radio Access Technologies (RATs) – HSPA, LTE, Wi-Fi or other novel RATs - would be leveraged to interface mobile devices to the cloud to achieve best area spectral efficiency (b/s/Hz/m2) This will make all the standard wireless attacks like Wi-Fi sniffing, DoS attacks, address impersonation, and session hijacking applicable to the wireless access network [1].

SDN controllers, network devices and the servers providing cloud services by a combination of cloud servers, data storage systems, virtual machines, hypervisor and protocols will be central to 5G infrastructure. The major threats to servers and clouds are Virtualization, Network Slice security, Improper Access Control, data-replication, Roaming Partner vulnerabilities, DDoS & DoS attacks, etc [2,9,17]. The centralization of network control platforms in SDN will make it vulnerable to saturation attacks and DoS attacks. Inadvertent exposure of the critical Application Programming Interfaces (APIs) to unintended software, might impact the entire network operations. Before 5G networks, mobile networks had dedicated communication channels based on GTP and IPSec tunnels. The communication interfaces, such as X2, S1, S6, S7, [18] which are used only in mobile networks, require a significant level of expertise to attack these interfaces. However, SDN-based 5G networks will have common open SDN interfaces and that will increase the attack surface. Further, TLS (Transport Layer Security)/ SSL (Secure Sockets Layer) sessions being used to protect the three communication channels- data channel, control channel and inter-controller channel- in the current SDN system, are highly vulnerable to IP layer attacks, SDN Scanner attacks and lack strong authentication mechanisms [5]. The dynamic nature of Virtual Network Functions (VNFs) may lead to configuration errors resulting in security lapses like the whole network can be compromised if the hypervisor is hijacked. Virtualization will make the systems more vulnerable to intrusion attacks with the motive of monitoring or modifying the platform or simply running software routines while remaining undetected [17].

Due to massive connectivity, user and data privacy will become more challenging to achieve. The major privacy challenge for a user remains same – identity, location and data- as in previous generation networks and attacks like IMSI (International Mobile Subscriber Identification) caching and signalling based attacks remain applicable here [18]. However, whereas in the previous generations, mobile operators had direct access and control of all the system components, in 5G, operators have direct control of neither the network nor the data. The network infrastructure will be shared among various operators – all using the services of Communication Service Providers (CSPs). Various 5G operators will have only virtual networks which in turn utilize the same network infrastructure. Data storage will also be in cloud environments using shared servers and services separated only by NFV with no physical boundaries. The strong possibility of user data being stored in a cloud in a different country will challenge privacy requirements further.

UE, as an endpoint, has the applications running and necessary interfaces to access networks and clouds and is vulnerable to the application threats arising out of malware, spyware used by the adversary to either disrupt or extract sensitive user information. Other attacks on UE can be MiTM, DDoS, Device tampering, sensor susceptibility [10].

Fang, Quan and Hu [1] have provided a glimpse of security services offered in 5G networks - authenticity, availability, confidentiality and integrity. Authenticity, until now, is catered in the cellular networks by mutual authentication of the UE and MME (Mobility Management Entity) of the network provider [18]. Due to the HetNet, low latency, energy and spectral efficiency requirements in 5G, message authentication and entity authentication will become more challenging. In [9], authors have argued that authentication can be provided either by networks only, service providers only or by both network and service providers in 5G. A new Authentication and Key Agreement (AKA) scheme for entity authentication are proposed in [11]. An interesting low latency message authentication scheme is proposed by authors in [12]. For Availability, Spread Spectrum (SS) Techniques like Direct Sequence (DS) and Frequency hopping (FH) are used extensively to prevent jamming, as a physical layer security measure [1]. SS increases the bandwidth of the signal either by spreading the user signal below the noise level using special codes in DS or by changing the instantaneous frequency of transmission quickly using a pseudorandom sequence, making it difficult for the adversary to tune their jammers. Time-hopping DS method is proposed in [13] over the normal DSSS methods, as this will have a higher probability against adversarial jamming. Data Encryption prevents leakage of information to the adversary from the broadcast information and its strength depends on the underlying crypto algorithms. Symmetric key cryptography is still used for data encryption and the secret key is either pre-shared between communicating parties or derived as part of session establishment during the authentication phase. Due to massive connectivity, privacy service is very important in 5G networks compared to cellular networks in the past. Special privacy algorithms are proposed by authors in [14], [15] for location and identity privacy. Authentication techniques provide guarantees against the source or origin of message or entity but do not prevent modification or duplication. Integrity comes in here. The integrity keys are derived during AKA [16] and are used throughout communication to prevent undetected message manipulation.

The security aspects of the 5G system as specified by the 3GPP are presented in their paper by Ananda et al [19] and also by Zhang and Kunz [20]. The security features, mechanisms and procedures performed within the5G systems are highlighted in 3GPP Security Association (SA) release 15. Mutual authentication of UE and network was introduced in 4G however, in 4G the Subscriber Permanent Identifier (SUPI) was sent in clear leading to privacy attacks. In 5G, SUPI will be encrypted using Elliptic Curve Integrated Encryption Scheme (ECIES) and the Home Network's (HN) public key (which will be stored in the UICC in USIM) even before AKA (Authentication and Key Agreement) [19]. Also one more difference in proposed 5G authentication scheme compared to LTE is - dual authentication requirement; whereas primary authentication is similar to LTE where the device is authenticated by the service provider network when it accesses mobile network services; the optional secondary authentication will be done to an external data network (DN), if so desired by the external DN, to provide services security. Further, during roaming HN had to trust the visited network through which authentication took place, but in 5G, HN will receive a proof of UE participation in successful authentication, reducing the fraudulent cases [19]. Additionally, in 5G, Security Protection Proxy (SEPP) will be used to interconnect control planes of the home and visited network to prevent different attacks like key theft, re-routing attacks in SS7[21], network node impersonation and source address spoofing [22]. SEPP provides application-layer security (confidentiality, integrity, replay protection, mutual authentication, authorization, key management, cipher suites negotiation, topology hiding and spoofing protection) for all service layer information exchanged between two network functions. In 5G, the RAN is separated in Distributed Unit (DU) and Centralized Unit (CU) - together they form 5G base-station (gNB). The messages between DU and CU includes control plane, management plane and user plane traffic over the F1 interface and hence Confidentiality, Integrity and Replay Protection are to be catered for the F1 interface. The standard has provisioned for security between 4G and 5G networks interworking as well to give a migration path. Various scenarios of dual connectivity where the UE will be connecting to LTE as well as New Radio (NR) are described in [23]. Security solution for the mobility from 5G to 4G networks w.r.t. the two handover conditions – UE in active mode and idle mode- are described in [24]. In both, the cases mapped security context is derived for secure service continuity, which is a derivation of the 4G key from 5G. Other than the above standard cryptographic techniques, new techniques like power control, relay, artificial noise and signal processing are some of the other techniques mentioned by in [1] to provide security to 5G networks.

In [2,9], the need for a different approach for 5G security is stressed upon due to the vision of 5G to serve service verticals more than just providing higher throughput to humans. Traditional security of UE, network authentication and hop by hop encryption will not be sufficient due to IoT. In IoT, people will talk to devices from their UE and hence stronger authentication techniques are to be devised. Similarly, different services will have differentiated end to end security requirements like stringent authentication is necessary for heterogeneous networks but it must also meet the ultra-low latency requirements, especially for services like autonomous vehicles.

The basic premise of security services has remained unchanged over the years. Confidentiality, Integrity, Authenticity and Availability are the key tenets of security from the beginning. However, with the ubiquitous deployments and varying form factors of connected devices and their capabilities, the adaptation of the suitable security solutions has become a challenge. For Eg. Whereas IoT devices will be looking for lightweight cryptography to save energy spent on complex computations, the enhanced mobile broadband-based applications will be looking for very low overhead cryptographic solutions to provide the promised Gigs of bits/sec and on the other hand for the mission-critical applications, reliability and low latency precedes over any other features and hence fast/quick computational algorithms will be the need. With the increasing virtualization and programmability, as in NFV and SDN, maintaining the integrity of the underlying hardware, checking the authenticity of the new configurations in real-time becomes one of the key security challenges.

4. Application of 5G in Military Communications

Military strategies rely on reliable, secure, quick communications and 5G technology will enable remote and reliable connectivity, reduce latency, energy-efficient and will have wide bandwidths. All this will enable relaying of a life-threatening situation in the theatre of operation possibly reducing fatalities in the war zone. 5G will also improve the information sharing within the various fighting groups, with secure and reliable video sharing using bodycams and location sharing [31]. Enhanced connectivity of sensors, robots, vehicles, troops in remote locations will reduce the response time in case of emergency and enable quick delivery of necessary supplies – ammunition, food, medicines etc - to precise locations through 5G connected Drones. 5G technologies will enable better data collection on material usage and hence will positively impact the future supply chain and military budgeting. [31]. With IoT, military communication devices will provide fast close-range communication using D2D communication without requiring satellites relays and thus reducing the cost of military operations, according to 2017 report in China Defence News [32]. the, 5G components needs to be suitably ruggedized and packaged as portable to be moved around. [30]. Also, suitable mechanisms in terms of enhanced processing or different cell architecture will be required to compensate for the higher losses of mmWave signals.

Some of the future battlefield scenarios that are leveraging 5G technology along with IoT as described by Liu Zhen, in the South China Morning Post on January 2019 [25], are reproduced below.

4.1 Machine-to-Machine Communication

Zhen [25] has presented the use case of 5G technologies in a combat situation in some remote jungle very effectively. A group of soldiers are moving across the jungle during a skirmish all with smart wearable's that directly communicate to each other (machine-to-machine communication). The wearables are also monitoring various health parameters in real-time and any attack on the soldier is immediately detected by them. The wounded portion is protected by automatic tightening of the belt and maybe an injection of first aid. Simultaneously, the nearest emergency aid centre and the group members are alerted. Guided by location tracking devices on the wearables, auto-driven ambulance arrives for the injured soldier and reinforcement unit arrive in armoured vehicles to encircle the enemy along with remaining platoon.

4.2 Future Battlespace Scenarios

As per [7,28], hypersonic weapons, being built by USA, Russia, China and others will be ready by 2022. With the super high speed (15-20 times the speed of sound), intercepting or guiding them is beyond the scope of current generation networks. 5G networks, as envisaged at present, will have both the required BW and minimal latency. Moreover, these hyper glided vehicles (HGV) will be flowing at a much lower altitude to avoid being detected by Air defence systems and hence this lower altitude, might be within the low range capacity of mm waves of 5G networks, albeit with a slew of interconnected relays. With the lower latency and reachability (enabled by a network of relays – tens of thousands in a given periphery), 5G has the potential to provide real-time connectivity to these hypersonic weapons from ground stations as well as to detect them by the future air defence systems.

Zhen has presented a few science fiction scenarios in [25] wherein an aircraft carrier is simultaneously attacked by a missile as well as a torpedo. With the aid of on-board sensors, networked together and providing real-time situational awareness to the captain, a cloud of drones and swarms of autonomous underwater vehicles (UUVs) are launched by the captain. Drones form a barrier that deflects the incoming missile into the sea. And UUVs form barriers to intercept and destroy the inbound torpedo.

4.3 Perimeter Security, Telemedicine and many more – Creativity, not the technology will be a limit

5G will leverage millimetre waves spectrum where signal attenuates very fast thereby reducing the range significantly compared to the 4G spectrum of sub GHz. This property can be leveraged in two particular use cases for military installations A large number of sensors can be deployed across the perimeter due to available large BW and Ultra-low latency to provide perimeter security without the threat of enemies detecting the sensor communications[34]. Similarly, the use of a directional antenna and low ranges with high BW and Low latency makes 5G an ideal technology for communication among various command posts of a formation, without the threat of detection, jamming, eavesdropping etc. The mm-wave signals are prone to attenuation by buildings, foliage, moving objects etc. Therefore, 5G technology will leverage directional antenna with beamforming which will inherently provide anti-jamming properties. These properties can be leveraged in designing multiple layers of spectrum for different networks with no additional hardware[34].

5G technology also has the potential of making the concept of smart bases a reality. With the maturing biometric technology, the same can be deployed at front gates for automated and robust access control. Similarly, the real-time exchange of situational awareness data vis a vis available resources (manpower, weapons and ammunition, ration etc) at a base will definitely result in optimal deployment and distribution of weapons at the target, providing an edge in a theatre of operation.

Another critical application of 5G will be robotic surgery in a remote battlefield providing the prompt and best healthcare to prevent lethalities and disabilities.

5. Present Status of 5G Development

With the host of new technologies and potential applications in all aspect of life, many countries are in the race to become the first-mover in commercial 5G deployment within their territory as well as globally. Historically, the first-mover country sets the mobile standards resulting in millions of job creations and billions in revenue.

China, South Korea, the United States, and Japan lead the field and expect to deploy 5G networks by 2020 [7,26,29]. The testbeds are live in the United Kingdom, Germany, France and other European countries and they are expected to deploy 5G soon after. Singapore, Russia, and Canada also have made significant progress in this direction. The present status of 5G development and deployment across the globe is shown in figure 3 below [29].

India is trying to roll out the 5G services along with the other countries worldwide. Reliance Jio in India may be the first service provider to launch 5G services in India [29]. Indian Government has launched a project for building an End-to-End 5G Testbed comprising of 5G BS and UE nodes [27]. IITM/CEWiT is the lead of the project with several other IITs and IISc involved. The first version of the testbed would be ready by the end of the year 2019 and the final version of the testbed will be available by 2021.

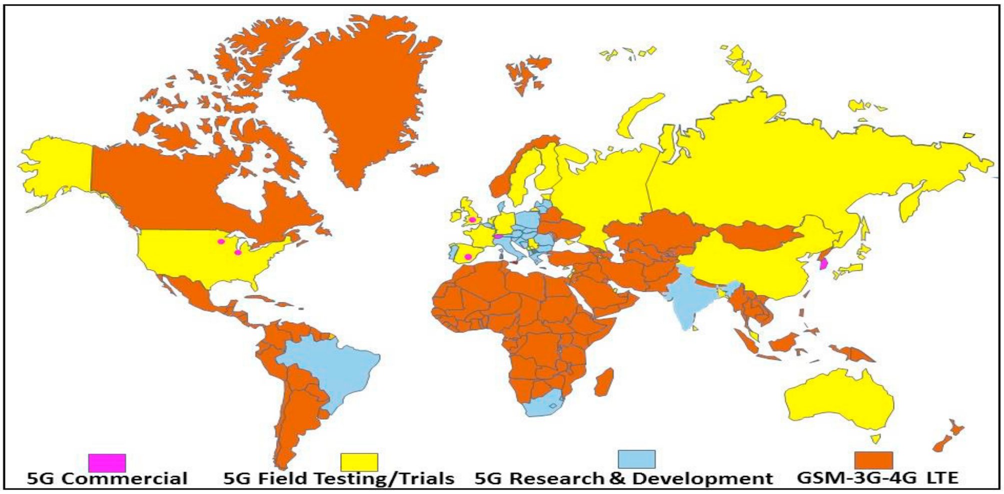

Fig. 3. 5G Rollout Across Globe [29]

6. Conclusion

At present the development of 5G networks is a work under progress, hence experimental data is not available in the open literature to validate the claims of its effectiveness in commercial and/or military domain. Notwithstanding this, the fact that 5G networks will be a leap forward in mobile communications with increased bandwidth, cannot be overlooked. This increased speed of data transfers will enable a host of new applications both in commercial and military worlds. Whereas the day to day life will be hugely impacted, in a positive manner, by a host of connected devices with on-board sensors, actuators and Artificial Intelligence (AI) algorithms, enabling autonomous operations and increasing efficiency in terms of management of resources and speedy delivery of services. In the military world, the availability of 5G networks will improve the situational awareness by transmission of large amount of intelligence, surveillance and reconnaissance (ISR) data in real-time to the commanders. This will not only provide an edge in the tactical environment during a conflict, but it would also improvise logistics and resource management during peacetime and otherwise [28]. Autonomous vehicles, smart cities / military bases, high BW, low latency applications enabling cloud-based services both for commercial as well C2 (command and control) environment are some of the overlapping usages of 5G networks.

However, the large number of connected devices and the network virtualization techniques for core infrastructure will definitely increase the potential attack surface. More dependencies on these networks have already made them part of critical infrastructure and any operational glitch (due to a bug or malware) will result in a catastrophic effect on the society as a whole.

India always had a huge dependency on foreign equipment (base stations, routers, servers, handsets etc) for the deployment of mobile networks. Most of the companies, be it USA based or of Chinese origin, are tied to their local laws to co-operate with their respective National Security Agencies. Hence possibility of a backdoor in all these equipment to provide private data to their Governments cannot be denied.

The deployment of 5G networks is the need of the hour to meet growing demands and immense opportunities it would eventually provide. It is absolutely essential to work out network design with adequate security mechanisms built at each layer to make it robust enough to prevent an attack and also resilient enough to survive/recuperate from a successful attack.

References

[1] D. Fang, Y. Qian and R. Q. Hu, "Security for 5G Mobile Wireless Networks," in IEEE Access, vol. 6, pp. 4850-4874, 2018.

[2] White Paper “5G Security Innovation with Cisco” by Geller and Nair

[3] https://www.forbes.com/sites/stratfor/2018/04/03/the-u-s-china-and-others-race-to-develop-5g-mobile-networks/#79adafa25875

[4] ITU Workshop Algiers 2018- 5G- INES.pdf

[5] Fundamentals of 5G Mobile Networks, First Edition. Edited by Jonathan Rodriguez. © 2015 John Wiley & Sons, Ltd. Published 2015 by John Wiley & Sons, Ltd.

[6] M.Agiwal, A. Roy, and N. Saxena, “Next Generation 5G Wireless Networks: A Comprehensive Survey,” IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 1617–1655, third quarter 2016.

[7] The 5G Ecosystem: Risks & Opportunities for DoD Defense Innovation Board, 3 April 2019- https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF

[8] Fettweis, G. and Alamouti, S. (2014) 5G: Personal Mobile Internet beyond What Cellular Did to Telephony. IEEE Communications Magazine, 52(2), 140–145

[9] 5G security: Forward-thinking Huawei white paper," Huawei, Shenzhen, China, White Paper, 2015.

[10] https://simalliance.org/wp-content/uploads/2016/02/5G-Security-%E2%80%93-Making-the-Right-Choice-to-Match-your-Needs.pdf

[11] A. Zhang, L.Wang, X. Ye, and X. Lin, ``Light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems," IEEE Trans. Inf. Forensics Security, vol. 12, no. 3, pp. 662_675, Mar. 2017.

[12] E. Dubrova, M. Näslund, and G. Selander, ``CRC-based message authentication for 5G mobile technology," in Proc. IEEE Trust-com/BigDataSE/ISPA, Aug. 2015, pp. 1186_1191.

[13] N. Adem, B. Hamdaoui, and A.Yavuz, ``Pseudorandom time-hopping antijamming technique for mobile cognitive users," in Proc. IEEE Globecom Workshops (GC Wkshps), Dec. 2015, pp. 1_6.

[14] S. Farhang, Y. Hayel, and Q. Zhu, ``PHY-layer location privacy-preserving access point selection mechanism in next-generation wireless networks," in Proc. IEEE Conf. Commun. Netw. Security. (CNS), Sep. 2015, pp. 263-271.

[15] E. Abd-Elrahman, H. Ibn-Khedher, and H. Afifi, ``D2D group communications security," in Proc. Int. Conf. Protocol Eng. (ICPE), 2015, pp. 1_6.

[16] M. H. Eiza, W. Ni, and Q. Shi, ``Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks," IEEE Trans. Veh. Technol., vol. 65, no. 10, pp. 7868_7881, Oct. 2016.

[17] I. Ahmad and T. Kumar and M. Liyanage and J. Okwuibe and M. Ylianttila and A. Gurtov, “5G security: Analysis of threats and solutions,” in 2017 IEEE Conference on Standards for Communications and Networking (CSCN), vol., no., Sept 2017, pp. 193–199.

[18] LTE Security Second Edition, book by GuntherHorn, Dan Forsberg, Wolf_DIetrichMoeller and Valtteri Niemi. Published 2015 by John Wiley & Sons, Ltd.

[19] 3GPP 5G Security https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-800X_619.pdf

[20] X. Zhang, A. Kunz and S. Schröder, "Overview of 5G security in 3GPP," 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, 2017, pp. 181-186.

[21] Tobias Engel. (December 2014). “SS7: Locate. Track. Manipulate”, http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf

[22] GSMA RIFS: “Diameter Roaming Security – Proposed Permanent Reference Document”.

[23] NEC white paper, “making 5G a reality”, 2018, https://nec.com/en/global/solutions/nsp/5g_vision/doc/wp218ar.pdf

[24] Anand R. Prasad and Seung-Woo Seo, Security in Next Generation Mobile Networks: SAE/LTE and WiMAX, River Publishers, September 2011

[25] Real cleardefense.com/articles/2019/03/23/5g_and_battlespace_dominance_114276.html

[26] https://en.wikipedia.org/wiki/5G

[27] http://www.ee.iitm.ac.in/5g/ 5G Testbed

[28] https://www.techradar.com/news/how-the-5g-network-could-benefit-the-military

[29] 5G commercial network in 2019 world coverage map - 5G country list - 5G networks around the world - countries with world coverage 5G network technology country list.html

[30] https://www.mwrf.com/defense/bae-bets-use-artificial-intelligence-electronic-warfare

[31] https://www.cbinsights.com/research/5g-technology-disrupting-industries/

[32] www.scmp.com/news/china/military/article/2184493/why-5g-battleground-us-and-china-also-fight-military-supremacy

[33] https://www.everythingrf.com/News/details/5510-Global-5G-and-Military-Communications-Market-to-Share-Abundant-Technology-Crossovers-in-the-Futures

[34] 5G for WarFighters By Kimberly Underwood (June 1, 2019)