5

CYBER Security and Threats

The security challenges in communication networks are a major concern in today's world, with security threats and possible loopholes in communication systems appearing at much higher rate compared with technological advances in the communication systems in itself. Based on the operational structure of WISDOM 5G it is obvious to note the enormous security challenge that surrounds the overall operation of the network. Providing a unified access to the user and seamless migration between underlying access networks would necessitate enormous effort for securing the confidential data related to the user.

The security mechanisms to ensure reliable services utilized by the service providers rely on authentication, authorization, non-repudiation and confidentiality based mechanism among others. These mechanisms collectively ensure that service provider fulfil their liability to deliver reliable and trust worthy services. However, an underlying operational constraint of these mechanisms is the imposed latency. As WISDOM 5G requires almost zero latency for the user to access the services, it would be a major challenge to ensure reliable secure service and meet the objective of high data rate access to the customer in a ubiquitous manner.

Possible mechanisms that could be utilized for addressing the security challenges imposed on WISDOM 5G could be as follows:

Unique ID: Majority security mechanisms are initiated in networks to recognize a particular device in the overall network. If a given mobile device is recognized in a manner that differentiates it from other mobile devices then requirements for authentication and authorization could be avoided. Characteristics that could uniquely define a mobile device could be utilized for forming a unique ID.

Privacy by Design: Maintaining the data and user profile confidentiality is a major requirement imposed on the service providers through governing cyber laws. Security and privacy aspects are usually dealt with separate

comparison, with the other network operations. Designing of network components and the overall operational backbone in WISDOM 5G with privacy and security aspects as prime objectives could ensure reliable privacy and security.

5.1 Major Challenges Surrounding Future Cyber Security

The plethora of challenges that surround cyber security can be broadly categorized into the following broad areas:

5.1.1 Network Borders

The emergence of 5G network as stated earlier that merges cells of different sizes and allows unified access technologies for the user device would lead to disappearance of network boundaries. Further the user device is expected to directly communicate with devices that comprise IoT for acquiring information about a certain physical parameter. This would be a different operational setup from today's communication network wherein government entities, private enterprises and private individual users could be the three broad network categories. The government entities currently impose strict operational rules regarding their communication network. Large private enterprises also lay down operational regulations regarding their communication network. These operational regulations would be hard to maintain if the networks are unified and user devices seamlessly switch between them [1].

5.1.2 Hindrance to E Commerce

The intention to provide ubiquitous computing and communication capability with data rate is to allow users to access rich and diverse information unhindered. That would be supported with unification of access technologies and underlying networks, along with support for high mobility of the user device. It can be anticipated in future that many companies would roll out novel information providing services that required unhindered data rates. This will, however, be hindered if the user is prohibited due to a certain networks' rule and regulation, or the data connection is interrupted due to requirements for authentication and authorization. Cloud and Internet based service provider are looking at opportunities of the form such as [2, 3]:

- Anything as a service (XaaS)
- Sensing as a service (SaaS)

Large enterprises that provide cloud based and Internet based services wish to utilize the aforesaid data service models for increasing the utility of Internet and unification of networks that would comprise machines (IoT, sensing as a service). However, the concept is imposing massive operational complexities even on the enterprises as they are unable to figure out the possible way to deliver such a plethora of utilities and create business opportunity.

Therefore, it can be safely presumed that if the data delivery model is tough to design and operate, security and privacy challenges that such a unified network would throw open would be much more complex to address.

The unified network operation promises to offer the end user the enormous utility of high data rate access with ubiquitous connectivity and extremely rich access to required information. The enterprises also seek to tap into the huge business potential that such a unified network could offer. However, a major privacy and security invasion issue for the common users could easily occur in such a densely connected network could lead to the governments imposing strong prohibitory orders that could ruin the economy and business significantly.

5.1.3 International Cyber Disputes

The unified network in WISDOM based 5G would depend significantly on an Internet based core network. Currently, there is a major debate prevalent on controlling the Internet. As it has enormous power in the form of millions of people social networking using it, or the possible spying and cyber crime committed using it. Committing cyber crime with an intention to ally to harm a nation or a major business entity directly, i.e., cyber war is discussed in the following sub-section. Many countries want to have a multilateral control on the Internet, i.e., countries would have direct control on the Internet activities concerning them, including data servers that are related with them but situated in another land; while some countries want a major international entity to take control of the Internet. In both the cases there are possible restrictions that would be forced on Internet operations in future. To protect sovereign interests an individual nation is likely to regulate the Internet autonomy, but this could have detrimental effect on the possible services foreseen to be fulfilled in future through 5G. The more connected the world through a unified network would be, the harder it would be to govern it and bring about an international consensus on Internet Governance.

5.1.4 Cyber War

In a unified mega network that allows users to access information directly from cyber physical structures (CPSs) that are in place for automation and control of a CPS, the CPS could be attacked/compromised to harm the possible operations derived from that physical structure. Such attacks on CPS have taken place in current communication network scenarios such as Heart bleed and Suxnet. Their likelihood would increase significantly if the networks are unified and users gain larger uninterrupted access. In the event of a large scale, cyber attack could lead to paralysis of critical infrastructure services such as transportation and banking and public utility such as electricity distribution. The 5G communication network would bring the physical infrastructure and the cyber infrastructure very close, thereby the threats to CPS would be enormous.

The governmental agencies that currently have a tough task in maintaining public utilities security and government infrastructure protection could encounter a situation of securing the infrastructure manifold complex than it is today. Cyber defence similar to other conventional defence mechanisms are cost intensive. Nations could be forced to increase their spending on cyber defence, in turn neglecting other critical priority issues that need to be addressed [1, 6].

5.1.5 Differentiation of Legitimate Versus Illegitimate Activities

The unification of various communication networks and devices, and the possibility of accessing information from devices diversely spread across the landscape would make it harder to determine as to what would comprise as legitimate and what would be illegitimate activities. Based on users' preferences and choices, the service provider wishes to mould that service and application to meet the users' requirement. This is a well-established practice today. In future, especially in the case of service delivery model such as sensing as a service and anything as a service, the service providers would try to data mine about the potential user/customer from their person specific data. The companies are highly interested in inferring the customer as closely as possible, since this influences their business prospects. As person specific data would grow based on the interaction a given person holds with the myriad of devices around, it would be very hard to draw a permissible line of what could be used for analytics and service providing and what comprises personal data that requires to be protected to ensure the privacy of the individual.

5.1.6 Legal System to Govern Machine-to-Machine Interactions

The legal systems around the world are designed keeping in mind the needs of the society, ensuring that by abiding by the law the whole society is secured. This is also applicable broadly for the cyber laws that have been enacted by the various governmental bodies. However, not in the 5G communication scenario that would comprise communication between machines (M2M) and IoT. The machines and devices would communicate with each other for certain self-automated tasks based on local decision making/intelligence, this could bypass the involvement of any human being governing the information exchange and automated decision making. In such a case a compromised machine may exploit a connected machine for gaining information or utilizing it to carry out an activity for illicit purpose. If the crime committed shifts from a human being to a machine, it would be tough to enforce any governing law existent today. The legal rules as applicable to common public are drafted such that they are comprehensible to a layman in the broad sense. For example a layman can understand reading Internet privacy and security rules as to what is the ethical way of using the Internet. However, drafting such a regulation base for machines/devices is infeasible considering the fact that interactions between machines would take place in a highly complex technical way, which could vary from machine-to-machine and underlying communication medium between the machines protecting network.

5.2 Users Awareness

For efficient user expertise of maintaining the expected cyber discipline in navigating across the plethora of data available it would be necessitated to educate the users of the usage etiquettes on the connected network. This is of tantamount importance as in a unified mega network in the form of WISDOM/GIMCV it would be necessary for the users to ensure that they access the data in an appropriate manner, following the basic guidelines. Some broad user guidelines and awareness are as described below:

The end users must be aware of these minimum safety measures [4]:

- To install the antivirus and anti-malware solutions in order to protect the devices from various virus or malware attacks. This idea has proved to be an effective solution against malicious attacks.
- The end users must be vigilant of the peculiar activities or behaviours in their own devices.

- They must install the applications from the original developer. The sources must be trustful having legitimate contact information and website.
- They should prefer to choose the applications on the Internet with the maximum number of downloads.
- They should not access their accounts or any other sensitive data when using those devices in public.
- They must ensure the frequent update of their operating systems and other software of their devices.
- They should also install a personal firewall to protect mobile device interfaces from direct attack and illegal access.
- The mobile network operators (MNO) should also be helpful to the end users by providing a secure environment. They can install antivirus and anti-malware software to scan outgoing and incoming SMS and MMS to the mobile network.

In addition to these, application developers should ensure that the sensitive or private data is not being sent to the unencrypted channel, which means data must be sent through HTTPS or TLS networks.

In brief we can note important players in securing the mobile wireless ecosystem. They include [3]:

- Mobile network operators (MNOs)
- Manufacturers of hardware, including mobile devices, chipsets and network equipments
- Application developers and market places
- Operating system vendors
- Network service providers
- Support software vendors
- Wi-Fi hotspot providers, over-the-top (OTP) providers and other platform providers

Most of the mobile industries are investing millions of dollars for providing the cyber security solutions for the strong security in the future. From the aspect of mobile operating systems security solutions include [4]:

- Mandatory encryption
- Application certificates
- Permission list for installations

The successful delivery of the mobile security or cyber security solutions require an active participation of the entire mobile landscape of mobile

communication stakeholders, industry, Government, enterprises and finally the consumers.

5.3 Spectrum Related Security Issues in CRNs

As discussed earlier cognitive radio principles would be highly applicable to ensure reliable use of spectrum especially where the access would be relying on conventional cellular bands apart from the proposed use of mm bands. Security related issues that surround cognitive radio based networks are elaborated as below

The exceptional growth in the cognitive radio (CR) has attracted several researchers as this innovative concept has proved its potential worldwide. A CR network (CRN) should perform following functions [5]:

- To determine the portions of the available spectrum and detect the presence of licensed users when a user operates in a licensed band which is termed as *"Spectrum Sensing*".
- To select the best available channel which is termed as "*Spectrum Management"*.
- To coordinate access to the channels with other users (secondary users) which is termed as *"Spectrum Sharing"*.
- To vacate the channel when the licensed user is detected which is known as *"Spectrum Mobility*".

Some of the spectrum access related security issues concerned with CRNs are [7, 8]:

- *Masquerading of a cognitive radio node*: This threat identifies the masquerading of a CR node while collaborating with other CR nodes for CR functions: spectrum sensing, spectrum sharing, spectrum management and spectrum mobility. For example, a malicious device can send wrong spectrum sensing information to other CR nodes. The affected functionalities are spectrum sharing, spectrum sensing and spectrum mobility.
- *Selfish Misbehaviours*: During the channel negotiation process, a selfish cognitive node tries to gain an unfair advantage and try to improve its own performance. The channel negotiation process is done using the results from spectrum sensing and the fairness depends on the cooperation of the contending nodes. A selfish node may conceal the available data channels from others and reserve it for its own use. The affected functionalities in this case are spectrum sharing and spectrum mobility.

- *Hidden node problem:* This threat identifies the case when a CR node does not detect the user because of the obstacles. The consequence is that, it transmits the same frequency bands of the primary user causing harmful interference. The affected functionalities are spectrum sharing, spectrum mobility and spectrum sensing.
- *Jamming of the channel used to distribute cognitive messages*: This threat identifies the jamming of a cognitive control channel that is used to distribute cognitive messages in the CR network. This can be executed against an out-of-band or an in-band cognitive control channel if the frequency of the channel is known. The affected functionalities are spectrum sensing and spectrum sharing.
- *Unauthorized use of spectrum bands for Denial of Service to primary user:* This threat identifies the case where a malicious node or CRN emits power in unauthorized spectrum bands to cause Denial of Service (DoS) to primary users. The affected functionality in this case is spectrum sharing.
- *Malicious alteration of cognitive messages*: This threat identifies the alteration of cognitive messages that are exchanged in the CRN. The affected functionalities in this case are spectrum sharing and spectrum sensing.
- Eavesdropping: This is a common threat or problem in the wireless systems where the privacy of the data is communicated over the other systems. The eavesdropper may get the access to the exchanged content over wireless links like CRNs and then exploit the information against the network.

5.4 Summary

Addressing security and privacy challenges in respect to 5G would require excessive examination. In fact it can be concluded that reliable 5G operations would be unfeasible until suitable mechanism that would ensure dynamic operations with excessive high data rate and mobility could prevent cyber crime against user(s).

References

[1] ICSPA, Project 2020 Scenarios for the Future of Cybercrime–White Paper for Decision Makers [online], Available: http://2020.trendmicro.com/Project2020.pdf

[2] HP pursues 'sensing-as-service' [online], Available: http://www.eetimes .com/document.asp?doc_id=1257823
[3] Where the Cloud Meets Reality: Scaling to Succeed in New Business Models [online], Available: http://www.accenture.com/us-en/Pages/ insight-cloud-meets-reality-scaling-succeed-new-business-models.aspx
[4] Jorja Wright, Maurice. E. Dawson Jr, Marwan Omar, "Cyber security and mobile threats: The need for antivirus applications for smart phones", Journal of Information systems technology and planning, volume 5, Issue 14, pp. 40–60, 2012.
[5] Abdullahi Arabo, Bernandi Pranggono, "Mobile Malware and Smart Device Security Trends, Challenges and Security", 19th International Conference on Control Systems and Computer Science, pp. 526–531, May 2013.
[6] "Today's mobile cyber security", Blueprint for the future by CTIA.
[7] Gianmarco Baldini, Taj Sturman, Abdur Rahim Biswas, Gyozo G´odor, "Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead", IEEE Communicatons Surveys & Tutorials, volume 14, No. 2, 2012.
[8] Neeli Rashmi Prasad, "Secure Cognitive Networks", Proceedings of the 1st European Wireless Technology Conference, pp. 107–110, October 2008.