Design Challenges in Wireless & Data Networks: Security as Case Study (Course Report)

Technical Report · April 2018

Muhammad Usama

Design Challenges in Wireless & Data Networks: Security as Case Study (Course Report)

Muhammad Usama[1]
[1]Information Technology University (ITU)-Punjab, Lahore, Pakistan

Abstract

This report covers the design evolution, shortcomings, and future design challenges in wireless and data networks. Security is considered as a use case to describe current architectural and design issues in wireless and data networks. This report also covers the technical and socio-economic tussles in the current design. I have also purposed a new cognition cycle to improve the current state of the art in the wireless cognitive network, which involves radio sensing, state of the art machine learning, knowledge base, estimation and decision making. This new cognition cycle will ensure systems thinking based security architecture by incorporating knowledge base.

I. Introduction

"An inexpensive instrument, not bigger than a watch, will enable its bearer to hear anywhere, on sea or land, music or song, the speech of a political leader, the address of an eminent man of science, or the sermon of an eloquent clergyman, delivered in some other place, however distant. In the same manner any picture, character, drawing, or print can be transferred from one to another place." — Nicola Tesla

Modern wireless and data communication systems are a combination of different distributed architectures, which involves many underlying applications, technologies, and networking policies. The fifth generation of communication technology is expected by the year 2020. With this new networking generation different allied networking and computational regimes such as the Internet of things, pervasive computing, ubiquitous computing, approximates computing and approximate networking is expected to contribute in building towards the network of everything. Cost of computing and networking hardware is expected to decay exponentially and with that networking cost also decays rapidly. This massive transition and new networking regimes have got research community to think of new alternative networking designs for wireless and data communication. In this section, we will briefly introduce and discuss the issues in previous and current networking architecture. We will also provide a list of problems in current networking architecture. This section will also include the social and economic challenges for next generation networking architecture.

A. Design Evolution of Wireless & Data Communication Networks

1) Legacy Wireless Communication Network: Legacy networking architecture lacks the ability of cognition. They usually follow a strict rule-based policy in determining the allocation of spectrum resources, identification of transmission channel, interference temperature, and many other network related information. These rule-based systems, initially work fine for a small set of users with limited quality of service (QoS) requirements, but as the wireless network grows in the number of users and their service requirements these strict rule-based systems with no cognition ability were not able to deliver the optimal performance. The major reason for this failure lies in the ossification of the network design which did not allow the transmitter and receiver to learn from the dynamic environment and results in bad network performance, poor QoS and wastage of network resources.

2) Cross-Layer Wireless Networking: Communication systems were designed in a strict layered approach, where each layer performed pre-specified tasks and follows strict layering principals to perform these pre-specified tasks. The major shortcoming of this design was the lack of the operational information dissemination to other layers, which is a major hindrance in fulfilling the necessary architectural design requirements of wireless communication system. Another reason for this failure was the time-varying nature of the wireless channel. To overcome these issues a cross-layer designing approach for wireless network was used, where joint optimization of networking protocols across different layers and improved coordination among different layers was introduced. Fundamentally, cross-layer wireless network architectures are based on sharing the knowledge of physical and media access control (MAC) layer of the wireless channel with the layers above them. This information sharing solves the critical problem of resource allocation in wireless networking. The major problem with this design approach is its lack of dynamic behavior adaption of the wireless network (user diversity and different QoS demands of users) and this lack of adaption has a negative effect on the tradeoff between performance and interoperability.

3) Cognition Based Networking: The rapid expansion of the wireless communication and the Internet has resulted in a complex heterogeneous design, which requires the network to be capable of dynamically adapting from the surroundings for intelligent resource allocation and interoperability. The ossified legacy layered network design and the stringently bounded cross-layer architecture are not able to meet the diverse needs of the new era of wireless communication systems. To meet these challenges the idea of cognition is taken from psychology and implemented in wireless communication network design. This new paradigm was named as cognitive radios.

a) Spectrum Access & Utilization: Before moving ahead with cognitive radios we need to mention another major issue which causes the diversion from cross-layer design to a more intelligent cognition based design. This issue is known as spectrum access and utilization. The electromagnetic spectrum is a scarce natural resource, regulated by governments. The expected exponential growth in connected devices and proposed small densely connected topologies for upcoming communication systems, will have a disruptive effect on spectrum allocation and utilization. Similarly, rapid growth in the adaption of new communication technologies and reduced cost of access, for personal and corporate use has raised serious questions about the availability and utilization of electromagnetic spectrum. Federal Communications Commission (FCC) published a report in 2002, which is considered to be a very first document reviewing the 90 years of spectrum allocation and usage. This report characterized the potential issues in electromagnetic spectrum allocation and usage [1]. Utilization of electromagnetic spectrum is biased in terms of occupancy of frequency bands in the spectrum when we sweep the whole frequency spectrum, few frequency bands are vacant most of the time, few are partially loaded and rest of them are heavily loaded. This uneven distribution of frequency bands usage causes under-utilization of the electromagnetic spectrum.

According to the FCC report, under-utilization of the electromagnetic spectrum will be the most significant problem in future communication systems. Under-utilization of electromagnetic spectrum occurs due to two major causes namely: *traditional command and control procedures* and *fixed spectrum assignment policy*. This under-utilization leads to a phenomenon known as spectrum holes. A spectrum hole is caused when the primary user (a primary user is the one which buys the license form the regulatory body and regulatory body assigns a frequency spectrum for a geographical area for a mutually decided time) to which a certain frequency band is assigned for a certain time, does not utilize it completely.

In 1999 Mitola et al. [2], proposed a solution to this fixed spectrum assignment policy by utilizing the spectrum holes for secondary users (users with no spectrum license) opportunistically, this policy is known as dynamic spectrum access (DSA). Opportunistic behavior involves sensing the surrounding environment and adapting to the statistical variations to extract the best possible result. This sensing, reasoning and adapting behavior is known as cognitive behavior. By incorporating cognitive behavior, Mitola et al. [3], in the year 2000 purposed a new paradigm of intelligent wireless communication systems called cognitive radios, which has the ability of sensing the statistical changes in incoming radio frequency signals and making corresponding changes in certain network operating parameters. This reasoning and adaptive behaviour has two primary objectives: *highly reliable communication whenever and where-ever needed* and *efficient utilization of frequency spectrum.*

Cognitive radios introduced a sensing and reconfiguring approach in networking but this design approach has some serious issues, like detection of weak signals from primary users before sharing the spectrum with the secondary user. It required a tighter control over the secondary user to avoid interference and this control has killed the whole idea of opportunistic networking. To solve this issue a new intelligent sensing algorithm along with customized transceiver was required. Another major challenge is to manage the tradeoff between the censored radius of the primary user and interference power to avoid the shadowing. Similarly, dynamic nature of wireless channel and diverse QoS demands needed a revised rate and capacity adaption algorithms for cognitive radios to work. Cognitive radios proved to be a much better design than previous cross-layer or legacy wireless designs but due to aforementioned flaws in cognitive radios design, it was not very successful. But it paved a path towards intelligent wireless networking.

B. Design Challenges for Next Generation of Wireless & Data Communication Networks

Now lets take a look on the issues in current wireless and data network designs. Heterogeneity, complexity, and dynamic nature are the three fundamental properties of next communication generation. The communication architecture and the Internet were not designed to fulfill these properties. With the emergence of new technologies such as the Internet of things, multicore architectures and exponential social adaption of these new technologies have rapidly increased the complexity of the wireless communication systems. This has also increased the QoS bar for the applications to meet the QoE of the users. With all these new technologies, wireless communication and the Internet have become a bounded closed loop system with multiple tradeoffs and restriction to avoid multiple performance issues, but now these strict policies have become a bottleneck in designing next-generation communication systems.

1) Network Management: As mentioned earlier there is an exponential increase in new innovative applications of the Internet and wireless communication technologies but we are lagging behind in network management and this is very alarming given the expected number of connected devices and their diverse nature. Network management has lagged behind in innovation curve because of fundamental strict bounded internet and wireless communication system design. To meet the challenges of next-generation communication systems and connectivity requirements, we need to think a new self-organized network management systems.

2) Field of View of Protocols: Wireless networks and the Internet employs multiple protocols to make communication between transmitter and receiver possible. These protocols are limited in their field of view and information sharing abilities with the complete network. Whenever we need to integrate a new system, we introduce a protocol in the software and then keep on updating the protocols to fix the raised issues due to variable network conditions, users QoE and security reasons. Although we employee all these fixes still we are lagging behind in user QoE, applications QoS, security etc. This is because the problem does not lie in protocols. It lies in the protocols limited field of view and their inability to model holistic network systems. Due to shortcomings, the operators are not able to have a complete picture of what is happening in the network. This causes multiple technical issues at the operator which also reflects on consumers QoE. Although network function virtualization, software-defined networking, and centralized control have offered a solution of the protocol problem, but apple does not the apple doesn't fall far from the tree. These schemes have their shortcomings and these shortcomings have their basis in rule based switching of SDN and closed form of networking. So in order to design next-generation networks, we need to increase the field of view of a network protocol and rethink the restriction on the coordination among the networking protocols.

3) Measurement & Quantification: Measurement and Quantification process of the wireless communication systems and the Internet is of critical importance. It is used for network planning and resource allocation. This process is usually decoupled from network control and performed offline and this is a major shortcoming in current network design. Since most of the next generation networks are considered to be self-organized, they need measurement and quantification process to be real-time and distributed to get a better view of network statistics to make an intelligent decision.

4) Knowledge Base: Current wireless communication and data network architectures mostly use rule-based or threshold based decision-making strategies, for their operation, automation, recommendation, and troubleshooting process. Very few applications such as SDN, employees artificial intelligence (AI) for decision making. When we consider designing a next-generation communication network, this lack of adaption of intelligent machine learning techniques in current wireless and data communication networks is a very alarming problem. The adaption of AI in networking along with centralized control and strong network analytics forms a knowledge base and provides the ability of real-time inference, which is a fundamental property of self-driven future networks.

5) Tussles: Current networking architecture has a distinctive per-hop behavior (for example routing). There are many parties involved in how to per-hop behavior should look like. These parties have their own agenda or function that they need to fulfill. These agenda can be aligned to the network overall function or these agenda have an adverse nature to optimize the network behavior to its own advantage without caring much about the overall system. This property is termed as Tussle [4]. Tussles have its basis in different social, political conflicting interests, biased users preferences, Internet service providers (ISP) monopoly, topological conflicts, competitive nature of the current networking business etc. These tussles will act as key enablers for rethinking the current networking architecture to support the future networking business.

6) Operators Wishes: The service provider or operator in current wireless and data network architecture is responsible for all the network planning, decision making, configuration, operation & maintenance, and measurement & quantification. Given the number of tasks and the expected number of connected devices in near future, this becomes a design flaw. We can leverage the advancement of machine learning, formal methods, programming languages, big data, genetic algorithms, approximate computing and approximate networking to offload the operator by introducing a sensing, collecting, adapting and reconfiguring property in the network devices and the end users.

7) Routing: Routing is a core part of any communication network, which provides the information flow in inter and intra-autonomous networks. These routing and forwarding algorithms are built on a strict non-adaptive policy which causes inefficient resource utilization. Routing and most of the network components follow strict rules this is because communication and data networks were not initially thought of as dynamic systems. Future communication networks are considered to be heterogeneous, complex and dynamic, so to meet the requirements of the future networks, a new self-aware and organized routing policy is needed.

8) Security: Another aspect of current networks which will be a major concern in designing the future network design is security. The security in wireless and data networks is ensured by using hardware firewalls, encryption techniques, and third-party inclusion. The Major goal of security in the current design is to make the best security possible to avoid any breach, but best security is not the perfect security. Best security solutions which include a combination of encryption and anonymization makes operators job of network management more tedious. We need to revisit the tradeoff between security and network management. Cognition-based solution by developing an intelligent model using the big data produced by the network can form a sustainable security solution, which not only satisfies the privacy concerns of the consumers but also makes network security management possible.

9) Optimization: "Premature optimization is the root of all evil." — Donald Knuth

In current network architecture network administrator or network controller (in case of SDN) performs networking parameters optimization operation to meet the diverse user demands and dynamic channel conditions. Current networking architecture has a complex multi feedback loop alike architecture and this property limits the field of view of the administrator or controller and results in premature optimization. This kind of optimization causes a disruptive effect on overall networking architecture.

10) Signalling Overhead: A very imminent threat for the next generation of communication networks is the signaling overhead this is a concern due to a large number of connected communication devices forming a heterogeneous architecture. To overcome this threat, a new alternative intelligent signaling design is required for future networks.

11) Connectivity vs Data Rate: In upcoming years embedded devices will cost less than one dollar and the number of connected devices will increase exponentially, this will cause a unique problem where instead data rate, connectivity will become a major problem. Future networking architectures must be able to deal with this issue intelligently, by making a smart connectivity policy.

12) Compromises & Tradeoffs: The current wireless and data communication network design is a combination of many tradeoffs, restrictions, and bounds, which is a problem when it comes to building a dynamic network architecture. These compromises are made to enforce a strict policy to ensure better resource allocation, improved resource utilization, optimal network performance, and security. The outcome of these compromises is not as they were expected, instead of producing optimal results in terms of avoiding breakdowns, security breaches, information loss, interference, and congestion these strict rules has proven to be shortcomings in designing a dynamic future networking architecture. Hardware and protocol design tradeoff, latency throughput tradeoff, the transmission rate restriction, the minimum and maximum frame size bound in TCP/IP stack etc are the few examples of the compromises that need to be revisited and improved for building an intelligent self-driven network.

C. Social & Economic Challenges

Two fundamental driving forces that had played an important role in the success of wireless and data networks are social needs and economic growth. These enablers are expected to be important components of future networks. Since the social and economic aspect of current networking architecture are key enablers, they are also considered as major challenges for future networks. We will discuss these two daunting challenges in upcoming paragraphs.

1) Social Challenges: Networking is not about connecting devices that share information it is about connecting people. The Internet and other communication networks were designed on the basic principle of sharing knowledge and meeting the social needs of the society. As society evolves the networking has tried to adapt accordingly by introducing different ideas such as congestion controls to dedicated systems, password protection to encrypted machines, spam filtering to firewalls, open network to regulated network etc. Given the social evolution, these aforementioned ideas may not work for future networks.

For designing new networking architectures, the research community has to look into these five fundamental social aspects.

(i) Do we need to revisit the social human contract which talks about the political and moral evolution of the human with time?
(ii) Do we need to provide cyber education to the community?
(iii) Do we need to conduct social studies to learn about the communication demands and risks before developing new designs?
(iv) How to convince the community to utilize the network for economic activity?
(v) How to settle on a less strict tradeoff on censorship and privacy, for keeping the idea of *Openness of Internet* alive?

2) Economic Challenges: The relationship between alternative networking architectures and economic viability is a very critical problem that has been ignored for too long in networking research. The infrastructure cost is decaying so does the communication cost how to build an economically viable new networking architecture. Economic problem will act as the most important problem and overshadows all the issues given in I-B [5].

There are ten fundamental questions that needs to be answered before designing the new networking architecture.

(i) How to build an architecture that routes money, packets are side effects?
(ii) How to deal with the fundamental tussle between ISP and regulator to get to a solution of how to utilize the infrastructure?
(iii) How to achieve the optimal longevity by keeping the economic growth?
(iv) Infrastructure should be owned by public sector or private?
(v) What are the incentive that can be offered to the private sector to keep them interested in investing the money?
(vi) There are about 5000 ISPs, are they willing to invest in new architecture?
(vii) How can we design a viable economic plan for bringing in the money from consumer? Is building smart markets, zero ratings and service specific billing a appropriate solution?
(viii) Should we put the regulations on networks and give its control to the state authorities to ensure trust guarantees and certificates? How this will affect the economic circle?
(ix) How to deal with local regulators?
(x) How to deal with the tussle between network cost and computing cost?

D. Rethinking the Networking Architecture

Given the problems associated with evolution of networking architectures and all the design flaws in current networking architecture along with social and economic issues, current networking architecture will not be able to support the diverse needs of upcoming communication systems. We need to rethink the networking architecture, which has the following properties fit to its purpose, secure, resilient, economically viable, manageable, intelligent, self organizing and meet the needs of society. Design evolution flaws given in I-A and issues in the current networking techniques provided in I-B invites us to rethink the networking architecture. In this paper we will try to provide an alternative design approach for meeting the challenges of next generation of communication networks by keeping in view the social and economic challenges mentioned in I-C.

E. Organization of the Report

In this report, we will discuss the a detailed review of all the key components of an alternative networking approach will be discussed which is based on improved cognition cycle. Section II discuss the design flaws in the security section III highlights the barriers to better security design. Section IV will provide basic details of new cognitive wireless network design and improved cognition cycle. Section V will conclude the report.

II. Security

In this section, we have discussed the issues and challenges in security architecture employed in current Internet and communication systems. Current Internet architecture has a very poor security architecture. It is a combination of many compromises and tradeoffs. Moreover, initial security design assumption were flawed. We will discuss these assumption and present how these underlying assumption resulted in a bad security architecture, but before that we need to look at the various definitions, perspectives and players involved in current security design.

Security in the Internet and communication systems had multiple definitions and they are all right in their limited scope. Initially security was defined as a system which performs only pre-specified tasks and avoid accepting or interacting with unsafe or vulnerable system. This definition of security does not fulfill the needs of modern Internet and communication systems. This is because the Internet or current communication systems have multipurpose and multifunctional characteristics. Pre-specifying the tasks of these systems will limit the utilization of these systems and this is not desirable. Moreover there are many unspecified tasks of the Internet and communication systems. Security architecture was not designed to meet these diverse tasks. Designing a security architecture for upcoming generation of the Internet and communication systems will be a very big challenge.

Consumers definition of security is very different from the aforementioned definition, consumers do not care about the specifications, technological advancement, physical limitations of device etc. They only require a security which has negligible probability of evasion. This makes security designers task more difficult. Another important aspect which is also relates with the consumer security definition is the tradeoff between security and privacy, it is a special case of the tussle between service provider and users. This tradeoff has not been handled properly in current communication and Internet design this section will also discuss the issues and perspective solutions related to security and privacy tradeoff.

Another definition of security is influenced by the economics and politics, where security is defined as a cost effective system which is not only used for defence but sometime use for offence. Different couturiers have different legal, social and economic laws and they influence the security architecture by imposing different restrictions and censorship. This biased approach has caused a serious concerns in security designing professionals. Designing the Internet and communication system security by keep the incentive for the investors and following the regional policies is another tradeoff that designers have to deal with. This section will also explains this important tradeoff.

This diverse nature of security definitions and related tradeoffs depicts that the initial goal of designing a general security solution was flawed and we need to reconsider the security architecture that can handle all the necessary security requirements of consumer, service providers, application developers, and regional authorities. To answer this question we need to understand two major concepts *Flaws in previous security design* and *Attack Characterization*. Flaws in previous security design will provide the initial design perspective and limitation details. Attack characterization is a process of learning the attacks dynamic behaviour and analyze it to form a defence mechanism against it.

A. Flaws in Current Security Architecture

In this subsection we will discuss the flaws in the Internet and communication system security design. We will follow a layered approach to describe the flaws in security architecture.

1) Physical Layer: Links, routers, server and many other related hardware constitute physical layer and it is highly vulnerable to the local and remote attacks using carefully crafted cyber tools and hardware. This layer also contains hardware related information, encoding and signaling, transmission and reception procedure and topological information of physical network design. Security architecture must ensure that this critical information stays private from unintended observer. Channel/links are susceptible to eavesdropping, active and passive attacks, adversarial attacks, information theoretic attacks and many other related malfunctioning.

Physical layer security of wireless system is bounded by two major imperfection of wireless channel namely fading and path-loss. There are other related wireless channel imperfections caused by nature but current physical layer security design was not developed by taking into account these wireless channel limitations. There are many security solution proposed to ensure security of the physical layer. These security solution are based on the coding theory, key generation, game theory, information theory and many other statistical and rule based schemes.

If we look at the service model and functional specifications of the physical layer they are ”best effort” and ”weak functional specifications” respectively. Best effort and weak functional specification means that hardware can malfunction, attacker can tape the channel for information, statistical approximation can go wrong, no service guarantees are offered to the users. These weak underlying design assumptions are the core reason of a bad security design for the physical layer. These weak assumption raise multiple unanswered questions like how to characterize the security, how to decide on a physical layer security design given the exponential raise in connected devices in upcoming communication generation, the security of physical layer is also related to the layers above how to ensure the security coordination.

Another related shortcoming in current wireless communication systems and the Internet which act as a limiting factor in designing an appropriate physical layer security is the concept of ”security as a service”. As mentioned at the start of the section that security has multiple dimensions and these dimensions will keep increasing as we get into the next generation of communication. In current security design for physical layer the security is considered as a service where hardware is placed in secure facilities and many coding techniques combined with encrypted key generation with trust sharing is used. All these security fixes are rule based, threshold based and context-less because the service base defence mechanism assume a uniform threat model. The major question here is how to develop a dynamic threat model.

Given all the aforementioned shortcomings in physical layer security we need to rethink the physical layer security for next generation of communication systems. We need to make the dynamic threat models along with intelligent coordination among the layers. This dynamic and robust physical layer security can be achieved by rethinking the cognition cycle and building a trust hierarchy based cognitive solution for physical layer.

2) Data Link Layer: Data link layer is responsible of moving packets from network layers to the host. Many attacks has been performed and proposed in literature ranging from address resolution protocol poisoning to authentication attacks on the wireless users. In wireless domain data link layer has faced many security challenges such as hidden node attacks, fake access point attacks, authentication attacks, MAC flooding, MAC spoofing, port stealing, VLAN hopping etc. Security in network is as strong as the weakest link, once the weakest link is compromised rest of the communication system will be compromised. In wireless communication networks and the Internet data link layer can be a weakest link. This layer is considered a possible weak link of security because this layer is not only attacked by the external attacker but also faces the insider threat challenge, where a rouge employee can share the insider information with the adversary.

Wireless channel has its own characteristics and these are exploited by attackers in deploying data link denial of service attacks where clear to send and request to send messages are flooded in the system which ultimately results in degraded quality of service. Similarly deauthenticaion attack where deauth frame is spoofed by the attacker because of low security results in disassociation of the user from wireless access point. This attacks depicts a fundamental security understanding flaw where the initializing frame security is compromised to ensure immediate connectivity. Another example of data link layer poor security is the fake access point attack, this attack is performed by spoofing the wireless beacon frames and intelligently crafting similar adversarial beacons and flooding the network with these adversarial beacons for the purposes of denying the connectivity to the legitimate user.

All the attacks and shortcoming explained are resulted because the current wireless data link layer model is just an upgrade of the wired data link layer model with multiple compromises to ensure wireless connectivity and availability. Data link layer security lacks the dynamic adaption from surrounding environment due to its static design and this results in flawed security architecture for data link layer. Since next generation communication systems are expected to be self organized we need to reconsider the data link security. We need to design data link security as a part of a trust based system which has the ability to defend against the adversarial and insider attacks.

3) Network Layer: Network layer is responsible for packet forwarding and routing through intermediate networks. This layer offers no service guarantees as it is based on best effort delivery. This underlying service structure causes lack of trust and coordination issues in developing security of network layer for next generation of communication systems. Network layer security is designed using IPSec protocol, where encryption strategies are used to provide data confidentiality and data integrity. This security works well but putting more encryption to secure data is not a good approach because attacker information will also get encrypted this reduces the probability of attacker detection and increases the complexity of network traffic analysis at the service provider end.

Another important task of network layer is routing, the current routing algorithms are does not possess the ability to learn from previous abnormalities and also lacks in technical security control. Given the expected heterogeneity and complexity of the future network these rule based and policy compliant routing algorithms does not fulfill the routing requirements. To solve this problem a new intelligent real-time traffic control scheme with trusted hierarchy support is required. Tang et al. [6] has proposed a new real time deep learning based intelligent traffic control system, this system is based on deep convolutional neural networks with unique input and output characterization for wireless mesh network backbone. Mao et al. [7] also proposed an intelligent routing method for future networks by utilizing deep Boltzmann machine algorithms. These new schemes are using deep machine learning technique but they have not considered security perspective of the network layer.

All these architectures and designs have to face two major challenges namely *trust hierarchy* and *migration problem*. Trust hierarchy is a scheme where communication entities uses trusted authentication mechanism via mutually shared like public key algorithm or trusted third party based authentication system. In future intelligent communication system this trust based network layer protocol is still an open research problem. Switching to new routing schemes with trust based authentication scheme at once will be very difficult at the global scale. This falls under the umbrella of social and economics problem. We need a new social contract with economic incentives for the users and service providers to switch to this new secure intelligent scheme.

4) Transport Layer: Transport layer is responsible for end to end communication in the network. This layer provides logical communication between application process running on different hosts. Transport layer provides synchronized, in order and guaranteed delivery with flow control and encrypted security. Previously it is possible to build a closed form tractable model of transport layer behavior because networks were simpler, rule based and less diverse. Future communication systems are complex and heterogeneous building a closed form behavior model to predict the change in the network is not a tractable solution [8].

Current security architecture of transport layer largely dependent upon cryptographic algorithms. Cryptography is a very powerful tool to ensure security but given the scale of the future networks this solution will become a hazard due to expected diverse security needs in future Internet and wireless communication systems. As we increase the number of devices, complex connectivity and multiple levels of security requirements cryptographic algorithms turns all the attacks on the different planes into an attack on availability and this is not desirable. Cryptography algorithms will not provide un-evadable security to the transport layer because of flawed end-to-end service model.

Transport layer also faces the session hijacking where an adversary hijacks the control on the session between two nodes. This is an attack on availability of the network and these attacks occurs because current wireless and Internet architecture does not dynamically learn from the previous information of session hijacking.

5) Application Layer: Application layer is the only layer which interacts with the users and provides full access to the user applications. In future networks application layer is considered to be the most crowded and problematic layer. User application design and its complexity is only limited by human imaginations, this causes a very serious security threat to this layer. The major security flaw in application layer lies in the diverse specifications of applications and their security requirements. There is no single threat model for dealing with this diversity issue. Another design flaw in application layer that limits the security of this layer is the lack of coordination with the other layers. Applications designers are not aware of security issues of other layers and this lack of coordination turns the diversity of application into a hazard.

Application layer security is also compromised due to social and financial conventions. It is application layer that defines how network will behave as all other layers are only responsible of their fix actions on the received packets. Many of the security risks we face now a days are due to bad design choices and compromises in application layer. Since applications are designed to facilitate the user requirements and this involves money. Applications developer does not take into consideration the security architecture of the whole communication or Internet stack. Today applications are designed to have more powerful functionality and features to raise finances, to do this developer takes security risks such as using active codes such as Java scripts and causes a communication and security risks. This application layer design approach is known as *insecure by design* and considered to be the root cause of the major security breaches in communication and Internet architecture.

III. Barriers to Better Security

The issues in current wireless and data networks security explained in section II. This section enlists the major challenges that network community need to solve to ensure better security for next generation of communication systems.

A. Self Organization

Self-Organization (SO) has been defined as learning from the environment and adapting the statistical variations in input stimuli to achieve highly reliable communications whenever and wherever needed. The growth in communication devices, data hungry application, and diverse security requirements has changed the focus of research community from static rule based security to dynamic learning security architectures. Since user behavior and user application requirements are only bounded by the human imagination, the underlying service architecture of current communication system is not good enough to cope with the dynamic security requirements of these applications. We need to build a self organization based security in each layer,to ensure a better security for next generation of communication systems. The desired security requires automated, real time measurements and inference on each layer and adapt accordingly to ensure consumers and operators trust on the security.

B. Tussles in Cyberspace

Current communication and Internet security architecture has different stake holders with aligned or adverse alignment of interests. Current communication and data network security does not take into considerations these tussles. Two Major tussles in security architectures are namely *user,operator, and governments* and *security and privacy*. Any security architecture design for the future networks have to deal with these tussles. *Design by choice*, *modulerization*, and *cognitive design* are the way forward in dealing with tussles. Design by choice involves offering more control to all stakeholders by designing an intelligent cognitive security architecture in the tussle space [9].

1) Tussle between user, operator, and governments: This tussle describes the adverse alignment of goals between user, operator and government. User want an un-evadeable security, operator wants more control on user traffic for QoS, traffic analysis and other network performance evaluation where as government want to impose their security policies and these policies are inline with their socio-economic goals. Current security architecture lacks in the ability of dealing with this tussle. Application of cryptography is a very related example to this tussle, as user uses multilayer encryption to ensure its security, operator does not want this level of encryption because this makes traffic analysis and detection of malicious user very difficult. Governments want a full control on user and operator operations to use security for user profiling, intelligence tracking and other related tasks.

2) Tussle between security and privacy: This tussle is a special case of user,operator and government tussle. This tussle has its roots is social behaviors. Current security architecture of the communication and data network was not designed by keeping in view the social needs of the consumer. Consumer normally confuses data security with privacy. Data security is related to confidentiality, integrity and integrity of the data, whereas privacy is related to right of personal privacy regarding the storing and usage of the user data. This tussle has turned into an arms race where users are employing different security techniques to keep their data private and operators are restricting them to ensure security of the network by detecting DOS and DDOS attacks. Another example of this tussle is the consumer profiling by different operators and consumer data selling to advertising agencies. This has been a major concern in networking community and network designers have to find a balance between security and privacy.

C. Lack of Systems Thinking

Wireless and data networks were designed is based on a Lego approach of learning. Where we optimize the network operations as separate entities. This optimization approach does not posses the ability of dealing with the requirements of future communication systems because this independent optimization can cause the unintended consequences on the performance of any other component in the system. For example major security problem in current wireless and data networks is due to the lack of coordination among the layers. for example, to provide powerful functionality application developer does not care for the security issues caused by the design choice made. Similarly greedy capacity achieving coding technique at the physical layer does not take into account the decoder complexity. For future network security should be designed as a system rather than as a service.

IV. New Wireless Paradigm

In this section we will present a new cognitive wireless networking design, which employees self organization and machine learning to overcome the shortcomings of current wireless and data communication networks mentioned in section I. This new design is based on the new improved cognition cycle which not only incorporate the sensing and adapting from surroundings but also involves the knowledge base to ensure systems thinking.

A. Improved Cognition Cycle

The cognitive wireless network is motivated by the shortcomings of current networking architecture, previous cross-layer network design and cognitive radios design. These shortcomings have their basis in increasing complexity, heterogeneity, and dynamic networking environments. To overcome these shortcomings, cognitive wireless networks are expected to be self-organized in future communication systems by employing new network design approaches, state of the art machine learning techniques, and improved cognition cycle. This self-organization can be achieved by introducing a learning and adapting mechanism in configuration, optimization and healing process. This complexity driven approach set the basis for designing the underlying theory of self-organizing networks, intent-driven networks, knowledge-based networks, software defined networks and many other intelligent networking architectures.

Cognitive wireless networks operation can be summarized in two steps namely *cognition* and *reconfigurability*. In sensing process, cognitive wireless network sense for wireless channel statistics, interference estimation, and event detection. These sensed attributes are then used for building an artificial intelligence in the network. Whereas reconfigurability stands for adaption of the intelligent decision.

- Analyze the radio channel and spectrum usage from surroundings.
- Intelligently reconfigure the network operation parameters to select the optimal frequency band for transmission.

Signal processing and machine learning techniques are used to provide cognition and software defined radio is used for providing reconfigurablity. Figure 1 depicts the new improved cognitive wireless network cycle, it also represents the core tasks of the major components and the information flow between these components.

1) Radio Sensing (Sensing): It provides the details about wireless channel sensing, network traffic statistics, interference detection/estimation, and observing an event. The raw information gathered in sensing process describes the characteristics of primary user spectrum. Radio sensing is also responsible for sensing the activity of primary users when the licensed spectrum is reclaimed. This activity sensing helps cognitive wireless networks in avoiding the interference and improve the overall end-to-end reliability of the network.
2) Knowledge Base (Analysis & Storage): In this step, the radio network telemetry for the primary user is performed, which involves event correlation, anomaly detection, performance monitoring, metric calculation, trend analysis, network semantics and many other related measurements. Knowledge base also records all the decision made in previous cognition and reconfigurability cycles, along with a set of available actions based on operator policy to improve the end-to-end network performance. Knowledge base combined with intelligent decision making act as a brain of the network which processes the

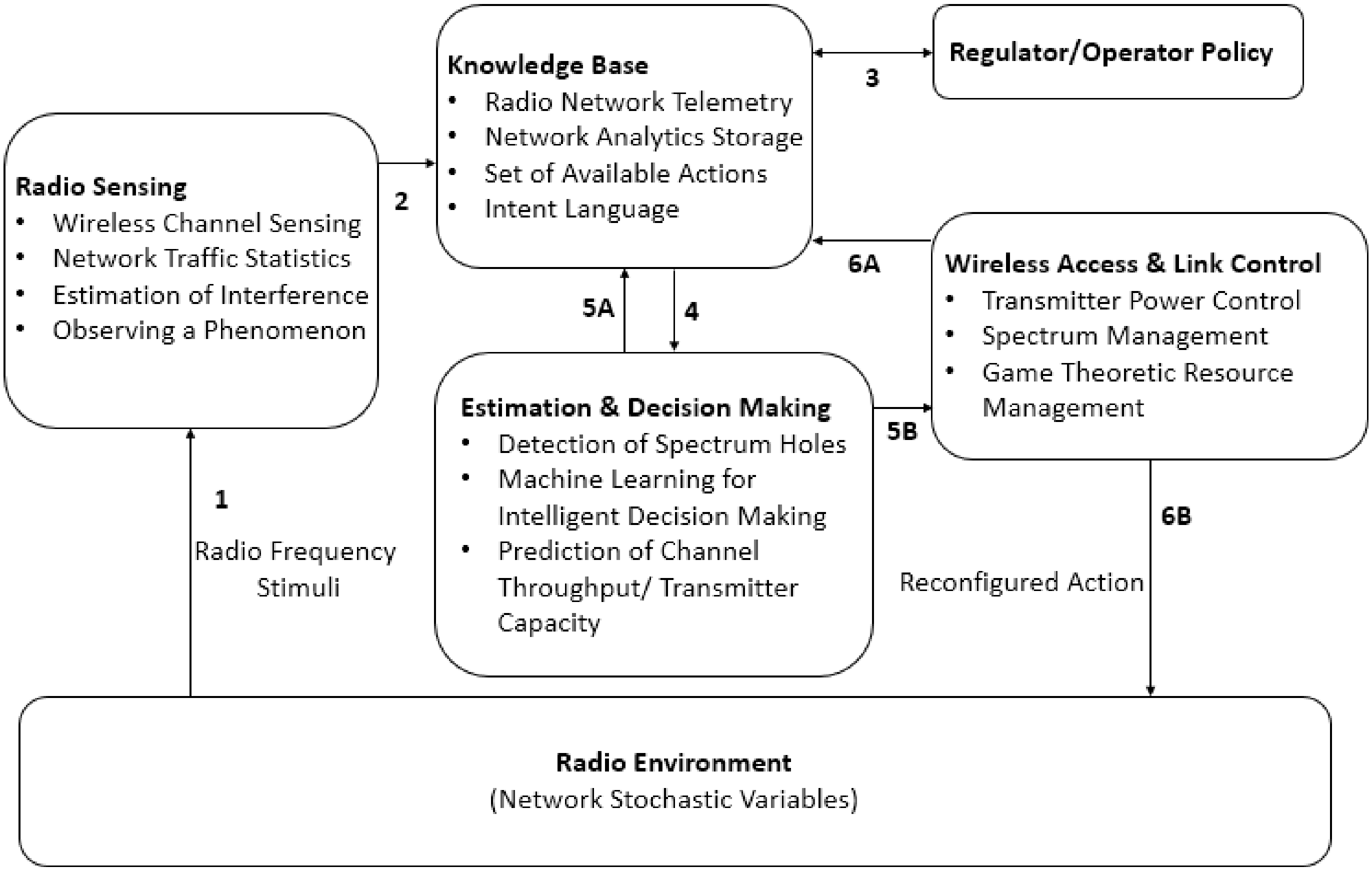
Knowledge Base
• Radio Network Telemetry
• Network Analytics Storage
• Set of Available Actions
• Intent Language
3
Regulator/Operator Policy
Radio Sensing
• Wireless Channel Sensing
• Network Traffic Statistics
• Estimation of Interference
• Observing a Phenomenon
2
6A
Wireless Access & Link Control
• Transmitter Power Control
• Spectrum Management
• Game Theoretic Resource Management
5A
4
Estimation & Decision Making
• Detection of Spectrum Holes
• Machine Learning for Intelligent Decision Making
• Prediction of Channel Throughput/ Transmitter Capacity
5B
1
Radio Frequency Stimuli
6B
Reconfigured Action
Radio Environment
(Network Stochastic Variables)

Fig. 1: Cognitive Wireless Network Cycle. (This figure highlights the major components involved in the cognitive wireless networking.)

sensed input and makes an intelligent decision. Estimation and decision making is another important component of the cognitive wireless network.

3) Estimation & Decision Making (Reasoning): This step involves the detection of spectrum holes based on the knowledge base information, gathered by sensing and processing the spectrum information of the primary users. Once the spectrum hole is detected a dynamic spectrum manager and handoff procedure enables the secondary user to pick the best frequency. This also involves machine learning for channel prediction, throughput/ transmitter capacity or any other customized intelligent decision making. With the evolution of deep learning and other efficient unsupervised learning techniques, estimation and decision making process in the cognitive wireless network has improved and in turn, improved the overall reliability of the cognitive wireless network.
4) Wireless Access & Link Control (Adapting): Estimation and decision making section, provides the information of channel prediction based on spectrum holes, transmitter capacity etc. Wireless access and link control section of the network implements the reconfiguration based on the provided information. A tighter power control is provided by wireless access and link control section in order to keep the interference caused by secondary users to the primary users and the interference among secondary users. Similarly, the competition for spectrum resource is also handled by wireless access and link control section by employing different game theoretic approaches.

Another very important element of the cognitive wireless network is spectrum mobility, which ensures the desired QoS of primary users mean while providing a resilient service to the secondary users. In cognitive wireless network spectrum mobility is defined as the process by which a cognitive wireless network user alters its frequency of operation for using the spectrum dynamically (allowing radio terminals to operate in the best available frequency band) and in case of primary user's reappearance, ensures a smooth communication to the secondary user with low latency during handoff process. Spectrum mobility and handoff process proved to be very useful in the multi-hop cognitive wireless network, where we need to relay and route information between dynamically changing channels.

The cognitive wireless network is a key enabler for next-generation communication technologies and due to its wide range of applicability it is a hot topic for research in academia and industry. It has many potential applications in wireless sensor networks, Bluetooth, emergency wireless networks, vehicular networks, smart grids. machine to machine communication, ad-hoc wireless networks and most importantly in 5G communications.

V. Conclusion

In this report, i have discussed the design challenges in wireless and data networks. I have discussed issues in the security of current wireless and data networking architecture. I have also proposed an improved cognition cycle which includes knowledge base to ensures systems thinking by incorporating advances in machine learning and big data. Future work will include the details of each block of the improved knowledge base and its application on security architecture.

References

[1] M. Marcus, J. Burtle, B. Franca, A. Lahjouji, and N. McNeil, "Federal communications commission spectrum policy task force," *Report of the unlicensed devices and experimental licenses working group*, 2002.

[2] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE personal communications*, vol. 6, no. 4, pp. 13–18, 1999.

[3] J. Mitola, "Cognitive radio—an integrated agent architecture for software defined radio," 2000.

[4] D. D. Clark, J. Wroclawski, K. R. Sollins, and R. Braden, "Tussle in cyberspace: defining tomorrow's internet," *IEEE/ACM transactions on networking*, vol. 13, no. 3, pp. 462–475, 2005.

[5] D. D. Clark, "Designs for an internet," 2017.

[6] F. Tang, B. Mao, Z. M. Fadlullah, N. Kato, O. Akashi, T. Inoue, and K. Mizutani, "On removing routing protocol from future wireless networks: A real-time deep learning approach for intelligent traffic control," *IEEE Wireless Communications*, 2017.

[7] B. Mao, Z. M. Fadlullah, F. Tang, N. Kato, O. Akashi, T. Inoue, and K. Mizutani, "Routing or computing? the paradigm shift towards intelligent computer network packet transmission based on deep learning," *IEEE Transactions on Computers*, 2017.

[8] N. Feamster and J. Rexford, "Why (and how) networks should run themselves," *arXiv preprint arXiv:1710.11583*, 2017.

[9] C. Kalogiros, A. Kostopoulos, and A. Ford, "On designing for tussle: Future internet in retrospect," in *Meeting of the European Network of Universities and Companies in Information and Communication Engineering*, pp. 98–107, Springer, 2009.