Emerging Network Technologies that are Likely to Become Widely Available in the Future.

Peter K. Kemei[1] and William P.K. Korir[1],
[1]Computer Science Department, Egerton University, Box 536, Egerton, 20115, Kenya
Tel: +254 727 725 372, Fax: +254 51 62527,
Tel: +254 727 725 372, Fax: +254 51 62527,

***Abstract*-- Emerging Networks technologies play an important role in the day-to-day administration of information technology in communications of different types of private and public networks. The emerging network technologies resolve the shortcoming of existing network architecture to enhance the facilitation of communication to the end user. These leads to adoption and improvement of some of the network technologies encouraging more innovation, research and development leading to emerging network technologies that are likely to become widely available in the future.**

***Keywords*—Networks, Computing, Wireless, Internet, Technologies.**

I. Introduction

Public computer networks have become an essential enabler for the communications on which most every-day to activities rely. Businesses in both public and private sectors are becoming increasingly dependent on information technology over all, and intra- and inter-organizational online communication and collaborations..

The availability, reliability, security and resilience of communication networks and information systems are vital to economy, society and security, communication and computing infrastructure resiliency is a function of *inter alia* technology, policy and the regulatory environment, economic interests, social relevance. There are network technologies, comprising one or more technologies that are currently in use or emerging within a few years, as having an impact on the networks. These technologies include cloud computing, real-time detection and diagnosis systems, future wireless networks, sensor networks, network coding, visualization of networks, semantic routing and cross layer design and optimization.

II. CLOUD-COMPUTING

Cloud computing technology is a new paradigm for obtaining computing resources and services. In a cloud computing model, computing resources, and processing power, software platforms and applications, are dynamically accessed through public and private networks. The key characteristics of the cloud computing paradigm [1] are composed of five essential characteristics, three service models, and four deployment models

A. Essential characteristics.

1. *On-demand self-service*: A user can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
2. *Broad network access*: capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.
3. *Resource pooling*: the provider's computing resources are pooled to serve multiple consumers using a multitenant model, with different physical and virtual resources assigned and reassigned dynamically according to users demand
4. *Rapid elasticity*: capabilities can be rapidly and elastically provisioned, in some cases automatically, from quick scale-out and rapid release to quick scale-in.
5. *Measured service*: cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service.

B. Service models:

1. *Cloud software as a service (SaaS)*: the capability provided to the user is to use the provider's applications running on a cloud infrastructure, cloud infrastructure, including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
2. *Cloud platform as a service (PaaS)*: the capability provided to the user is to deploy onto the cloud infrastructure user-created using programming languages and tools supported by the provider.
3. *Cloud infrastructure as a service (IaaS)*: The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

C. Deployment models

1. *Private cloud*: the cloud infrastructure is operated solely for an organization. It may be managed by the a third party and may exist on premise or off premise.
2. *Community cloud*: the cloud infrastructure is shared by several organizations and supports a specific community having shared concerns.

3. *Public cloud*: the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
4. *Hybrid cloud*: the cloud infrastructure is a composition of two or more clouds that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

D. Cloud Computing Applications and User Benefit

1. *Operational*: The highly scalable, virtualized nature of cloud services often implies a high level of redundancy and geographic distribution of the computing resources offered by the cloud services provider. The facilitation of rapid application development provided by cloud computing makes the deployment of new services and the expansion of existing ones easier.
2. *Financial*: Eliminating a significant portion of capital expenditure and moving it into operating costs optimizes business cost structure. Transferring some of the management responsibilities to the cloud service provider reduces operating overhead for the enterprise.
3. *Productivity:* Cloud computing embraces a shared, virtualized network computing environment, it has an

E. *Interests, Development and Adaption of Cloud Computing.*

The reliability of distributed systems depends on fault-tolerance and redundancy which provides the mechanisms for consistent data replication. Cloud caching guaranteed levels of connectivity. Offline service availability is important issues are that [2] there should be a complete copy of the relevant data, possibly regardless of its size, that [3] the data, as part of the service, should be secure, searchable, editable, and most of all synchronizable, and that [4] all the metadata that relates to the service and its running should be stored and usable when the user is back online. Seamless synchronization during online operations, combined with data replication and usage of alternative caching mechanisms is an appropriate solution to problem of occasional failures in connectivity.

Protecting sensitive data is essential. It involves ensuring that the data is available and can be accessed, its integrity is preserved and its confidentiality is preserved. Migrating computing applications to the cloud model, faces end-to end issues of trust.

Research is needed to identify gaps and effective solutions to increase the levels of assurance that can be provided through the cloud computing environment. Also research should be focus on data life-cycle management, process, and destroy data residing in the cloud; ensuring integrity of the cloud-based data, effective models for managing and enforcing data access policies and encrypted data storage that allows cloud-based processing capabilities so that cloud as an entity can be adapted fully and in future by user and business community since benefits are more than other existing technologies in terms of accessibility and reliability.

III. REAL-TIME DETECTION AND DIAGNOSIS SYSTEMS (RTDDS)

Detection and diagnosis systems is to detect faults, disruptions or decreases in the services provided due to intentional or unintentional actions, and to respond accordingly without severely deteriorating the network or system performance and reliability. The increasing velocity of malware spread through networks, detection is becoming insufficient if corrective action cannot be taken very rapidly. This raises the opportunity to explore machine-aided response and autonomic response.

The optimal detection and diagnosis system takes accurate decisions in real-time and respond promptly. Employing efficient real-time fault detection and diagnosis systems is of substantial importance to guarantee the resilience of the protected system.

Detection and diagnosis should be able to spot, the occurrence of faults, disruptions and decreases of the offered service's quality due to intentional attacks or unintentional actions (e.g. traffic peak events, network mis-configuration and fault scenarios that can be caused by power outages, physical damage to network or facilities, etc), and carefully assess the extent of the damage in individual components, so as to build a ''trust model' of the system.

RTDDS filter, process, and correlate information coming from a variety of sources e.g, network probes, application logs, firewall logs, operating system data structures, authentication logs, IP cameras, and virtually any sensor available in the network infrastructure in order to raise alarms, to trigger actions in remediation and to produce evidence for forensic use.

Resilient networks can be built over solid foundations, and one of the required building blocks is the capability of its operators to have situation awareness which refers to multiple technologies (algorithms, protocols, hardware) that cover a wide spectrum of network measurement, monitoring, detection, estimation, classification and identification technologies

A. RTDDS effects on Network.

RTDDS provide improved situational awareness and improve the resilience of networks by combination of intrusion prevention, detection and response techniques. Increased in autonomic security solutions, which combine sophisticated detection capabilities with automatic or semi-automatic response, will lead to efficient resilience of networks.

Autonomic security response is essential given the increasing sophistication of threats and the speed at which attacks can spread in networks. Where real-time detection functionality is part of a real-time prevention system sophisticated attackers can manipulate and confuse systems by causing valid and legitimate connections or messages to be rejected, by exploiting the response automatism leading lead to a crippling of the network that the systems were designed to protect. Emerging networked applications consisting of a high number of interconnected devices, such as the Internet of Things (IoT), would be expected to be under attack at all times.

Techniques should be developed which allow the overall system to continue providing a trustworthy service. The basic idea is that a system which is under attack can still deliver a service that is as trustworthy as the one it would deliver if it were not under attack, provided that: (i) the attack is spotted (*detection*) [5], (ii) the parts affected by the attack are clearly identified and the nature of the attacks is well understood (*diagnosis*)[6],and (iii) proper treatment actions are taken (*remediation*).Efficient *detection*, *diagnosis*, and *remediation* are thus key functions for achieving a trustworthy network.

B. Impact for efficient online detection and diagnosis

1. *Defy to mechanisms employed*: The effective development of a detection and diagnosis system that is able to minimize the false alarms while detecting unknown attacks, remains a challenging task. Detection approaches that make use of labelled data for training models of normal and attack behaviour cannot realistically function in the ever-changing environment of modern networks, where obtaining 'attack-free' or 'labelled' traces for training is extremely difficult since unknown attacks for which training data are not available at all. Investigation approaches that are able to detect attacks by using only normal, legitimate data has been proposed [7].The promising development of efficient RTDDS proper dynamical models as opposes to fixed time windows models. Technologies that constitute parts of RTDDS and that need further development are: scalable traffic measurement hardware and software, metrics for network health, and various detection algorithms. Sophisticated attackers disrupt or degrade the performance of the detection system forcing users to disable the detection and diagnosis systems [6].
2. *Defy due to of Network Size Increase and the Emerging Network Architectures:* The increasing scale of networks, due to the interconnection of small embedded devices with limited power, will make the problems of measurement and detection harder as the background noise and the quantity of information to be managed will rise. Scalable solutions and technologies are needed with higher efficiency, data compression and noise filtering. Emerging networking architectures is the collapse of backbone networks into Layer 2 networks (hybrid optical and packet switched) with limited Layer 3 functionality. This change might deeply impact the management and monitoring capabilities of network service provider. In scenario new lower layer network management technologies is require to solve the shortcomings. Increasing use of wireless communications where fault detection and diagnosis systems developed for wired networks cannot be easily applied to wireless communications due to the differences between these network types [9]. In wired networks, traffic monitoring is performed in firewalls, gateways, routers and switches. In Wireless networks lack of these types of network elements, making it extremely difficult to obtain a global view of the network. The loss or capture of unattended nodes or RFID tags may allow malicious adversaries to obtain legitimate credentials and launch sophisticated attacks. In case more new technologies has to emerge to limit the drawback exiting to current and future wireless enforce network security. Cloud computing may create a demand for RTDDS that are suitable for cloud service providers. to achieve high availability of cloud services will need RTDDS efficient in terms of detection speed, detection accuracy and response effectiveness. All these emerging networking technologies and future technologies requires efficient RTDDS to counter check network security alerts and monitoring.

C. Effectiveness of RTDDS

Raising false alarms carries a significantly lower cost than not detecting attacks. Cost-sensitive classification methods can be used in detection and diagnosis systems approaches [9] [10] & [11] relates to cost-sensitive intrusion detection.

1. *Real-time monitoring*: Accurate and timely detection, diagnosis, and remediation is achieved by gathering, filtering and correlating in real-time information which is available at the different architectural levels in network, operating system, DBMS and application [15].Dependable event monitoring and management facilities is the enabling technology to monitor networked applications in real-time. The accuracy of a detection system is increased by correlating data from multiple levels including network traffic scan, application events on server and client side, firewall /Virtual Private Networks concentrator events, identity and access control system events to make more informed decisions.
2. *RTDDS and inter-domain cooperation:* Developing situation awareness requires cooperation among operators. This cooperation will require an exchange of information and demand coordination between the operators. This cooperation will have to happen across national borders. An efficient way to incorporate policies in the cooperation process will be critical for the adoption of any proposed solution, as will be the question of sanitizing the exchanged data to limit the amount of knowledge about users, traffic and network structure extractable from the data.
3. *RTDDS v Privacy:* A privacy-preserving detection and response system should accurately detect an attack and respond to safeguard the performance and quality of the network. It should guarantee the privacy whose actions are monitored. In wired systems, privacy issues related to intrusion detection and response have already been identified [5], [6]. In wireless networks, privacy issues are more severe to payload data and context information like the location of a sensor node or an RFID tag. An approach proposed for the preservation of privacy in wireless sensor networks [7] and RFID systems [9].Important issue specific

for RTDDS is how fast queries can be performed to execute in a timely manner. RTDDS technology is important for safeguarding the resilience and reliability of communication networks will lead to more development and research of safer, more accurate RTDDS, provide real-world datasets representing network traffic. Security of the network is crucial for any user and organization in order to maintain integrity, confidence and availability of the network resource. RTDDS are essential facility to enforce the security policies and this technology is a requirement for existing and future networking technologies to be adapted now and in future both for private and public networks

IV. FUTURE WIRELESS NETWORKS.

Wireless network technology has changes the means of communication. It has become the significant option of any business because of its salient features like speed, security, mobility and WiFi hotspot. Voice application like Voice over Internet Protocol can be only possible because of wireless network. Wireless network has become the essential point of any network to make their customer more satisfied.

Wireless networks aim to provide acceptable service to applications, for mobile users and access of information when needed, maintenance of end-to-end communication, ability for distributed operation and networking.

A. Increasing the Robustness of the Networking Mechanisms

In wireless networking the main drawback is security features which attacks compromise the vulnerability of the network devices and systems.

The easiest way to mount DoS attacks against a network is to intervene routing protocol, the medium access control, the topology control and management, and channel assignment mechanisms to increase the robustness networking mechanisms.

Routing protocols provide proactive dissemination of routing information and local route computation, or on-demand route discovery, resource reservation on selected routes and error recovery during the data forwarding phase routing.

Information and route discovery requires the protection of the authentication and integrity of routing control messages. In order to protect them against manipulation routing information and route discovery requires the protection of the authentication and integrity of routing control messages, in order to protect them against manipulation minimize attack and promote the robustness of the networking mechanisms hence benefiting the end user and open new development opportunities in research towards development of future wireless networking technologies.

B. Radio Access Technologies(RAT) and Quality of Service QoS

Future wireless networks depend on radio RAT through the widely accepted notion of convergence in heterogeneity. It has be been envisaged as a convergence platform in which an all-internet protocol (IP) core network .IP core network could provide leverages to facilitate cognitive cooperation so that multimedia services can be provisioned optimally through the most efficient access network to anyone at anywhere, anytime.

The aim of future wireless is to achieve seamless mobility for end-users roaming between different environments and RATs, QoS, transparency support for demanding multimedia traffic consisting of real-time and non-real-time applications.

To realize these, the exploitation of heterogeneity within a multi-RAT environment is a starting point. First, no individual RAT has sufficient resources to meet the QoS requirements of end-users with varied multimedia applications. Second, end-users could remain `best' connected during the initial network access and also throughout the entire duration of their connection. Such always best connected concept [14] could be addressed by performing vertical handover (VHO) to the next `best' network that would satisfy the end-user QoS profile, delineating the need for adaptation to prevailing network conditions.

C. Vertical Handover (VHO) and Benefits

An optimal network selection technique [13] is the core component of cognitive co-operation. It directs informed VHO to exploit heterogeneity within a multi-RAT environment and optimize radio resource usage [12]. VHO will support seamless mobility and QoS transparency. Its chief advantages of permitting QoS-based handover, increasing the QoS satisfaction level of end-users, enabling network operators to integrate several RATs into a multi-RAT environment improving their coverage and QoS, improving trunking efficiency of networks through dynamic load distribution through the notion of cognitive cooperation. All these element enhance the benefits of future wireless networks technologies for the user and future advancement of the technology as more user and organization are adapting the wireless technology as means of communication and transmission since it is affordable and flexible.

V. SENSOR NETWORKS

Sensor network consists of spatially distributed autonomous sensors to monitor physical or environmental conditions. Sensor nodes small computers, in terms of their interfaces and components consist of a processing unit with limited computational power, limited memory, sensors and source of power. Wireless sensor networking is based on its construction.

Sensor network consists of small or large nodes called as sensor nodes. These nodes are varying in size and totally depend on the size because different sizes of sensor nodes work efficiently in different fields. Sensor networking have sensor nodes which designed in a typical way that they have a microcontroller which controls the monitoring, a radio transceiver for generating radio waves, different type of wireless communicating devices and also equipped with an energy source such as battery.

The entire network worked simultaneously by using different dimensions of sensors and worked on the phenomenon of multi routing algorithm which is also termed as wireless ad hoc networking.

A. Application of Sensor Networks.

In the present era there are lot of technologies which are used for monitoring are completely based on the sensor networking. Some of important applications are environmental monitoring, traffic control application, weather checking, regularity checking of temperature etc. Wireless sensor networks can also be used for detecting the presence of vehicles such as motor cycles up to trains. Some wireless sensor networking based technologies are in used in agriculture, water level monitoring, green house monitoring, landfill monitoring etc

B. Impact of Sensor Network

Sensor networking has important benefits include:

Store a limited source of energy, no hassle of cables and has mobility, can work efficiently under the harsh conditions, and it has deployment up to large scale etc. drawback insufficient speed of communication, it is to disturb the propagation of waves and hacking of networking and too costly to use.

C. Future of Sensor Networks.

Sensor networking has a bright future in the field of computer networking and emerging networking technology because it solves the monitoring problems at an advanced level in the future with the help of such technology of networking as more user are adapting and utilizing the sensor network as a means of communication and transmission.

VI. NETWORK CODING TECHNOLOGY.

Network coding is a method of optimizing the flow of digital data in a network by transmitting digital evidence about messages. The "digital evidence" is itself, a composite of two or more messages. The concept of network coding is an alternative to routing. In network coding, routers and switches are replaced by devices called coders.

Instead of directing the packets toward their ultimate destination, the coders transmit meta-data in the form of digital evidence about the message along multiple paths simultaneously. The meta-data arriving from two or more sources may be combined into a single packet. This distribution method can increase the effective capacity of a network by minimizing the number and severity of bottlenecks. In network coding, the data does not depend only on one transmitted message but also on the contents of other messages that happen to be sharing the route at the time of transmission. For this reason, network coding is more resistant to hacking, eavesdropping and other forms of attack than traditional data transmission.

The extent of throughput improvement that network coding can provide depends on the network topology and on the frequency and severity of bottlenecks.

In no event does network coding reduce the throughput compared with the routing method. Network coding may prove especially useful in multicast networks, wireless sensor networks, digital file distribution and peer-to-peer (P2P) file sharing.

A. Application of network coding.

1. *Network Monitoring*: Distributed Internet applications often use overlay networks that enable them to detect and recover from failures or degraded performance of the underlying Internet infrastructure. To achieve this high-level goal, it is necessary for the nodes in the overlay to monitor, assess, and predict the behavior of Internet paths, and eventually make efficient use of them.
2. *Operations of Switches*: Arriving data packets are stored in the input queues of the switch, and register a request to be forwarded to a specific subset of the output ports. To maximize the speed of operation, the switch uses a scheduling algorithm to serve as many packets as possible in parallel. the switch serves traffic flows, rather than individual packets. The packets in each flow have a common source and destination set and an associated arrival rate. To accommodate the multiple traffic flows, a technique typically used is speedup, which refers to that the switch operates at a faster clock than the incoming and outgoing network links.
3. *On-Chips Communication*: The design of Very-large-scale integration chips aims to simplify and minimize the length of on-chip wiring. Network coding can help reach this goal, at the cost of additional coding/decoding logic in the network. This overhead indicates that scenarios where network coding is beneficial may occur in the routing of multicast signals along long routes (buses).
4. *Distributed Storage:* Distributed storage systems store pieces of information entities (e.g., pieces of data files or sensor measurements) throughout the network, usually with the purpose to ensure sufficient storage capacity by using resources of multiple network nodes (e.g., disks at several computers or memory of wireless sensors). The information should be stored reliably over long time periods, i.e., with enough redundancy so that it could be recovered even if several of the computers or sensors were unavailable. Simple replication, a straightforward approach to storing data redundantly, is not very efficient in terms of capacity required to store the redundant information and transmission resources required to collect the distributed pieces of information. Networking coding is essential since it utilized network resources in efficient manner which increase throughput and proper utilization of bandwidth and other network resources. As emerging networking technology it is important in such a way that network infrastructure will be fully utilized and the make the technology to be adapted for future emerging network technologies as it important to use network resources efficient and minimize cost as the networks are become more complexity and dynamic.

VII. VISUALIZATION OF NETWORK

The operation of the different types of network and

Internet requires being able to monitor and visualize the actual behaviour of the network. IP network operators usually collect network flow statistics from critical points of their network infrastructure.

Flows aggregate packets that share common properties. Flow records are stored and analyzed to extract accounting information and increasingly to identify and isolate network problems or security incidents. While network problems or attacks significantly changing traffic patterns are relatively easy to identify, it tends to be much more challenging to identify creeping changes or attacks and faults that manifest themselves only by very careful analysis of initially seemingly unrelated traffic pattern and their changes.

A. *Application of visualization of network behavior.*

Network behaviour analysis plays on both the security and network operations sides of IT by collecting and analyzing network flow telemetry via Netflow, sFlow, JFlow, etc., to identify and remediate the cause of anomalous activity, such as traffic spikes, performance degradation and communication with unexpected IP addresses that might indicate botnet activity or data exfiltration. Understanding the cause of performance issues saves organizations from throwing bandwidth capacity at what appear to be network issue. Quick recognition improves time to resolution, saving money by bringing production systems back on line or to peak performance.

Visualization of network technology is important for user and business organization since it is indeed proper to be informed of activities and keep track of network architecture and functionality by visualizing day to day activities to be update so as to implemented actions necessary from the analysis and report after visualization of the network. This will help users and business community to utilize network resources efficiently and implement proper solution required. This network technology will be adapted by users and business organization since it essential in any network for fully utilization of network resources ranging from performance and security concerns as network are becoming more dynamic.

VIII. SEMANTIC ROUTING

Semantic Routing is a method of routing on the nature of the query to be routed than the network topology. Semantic routing improves on traditional routing by prioritizing nodes which have been previously good at providing information about the types of content referred to by the query.

In order to search for information on a peer to peer network semantically the data needs to have a semantic description associated with it, one popular solution is the use of RDF meta-data. Tagging documents/data with RDF would provide a rich 'semantic web' which could be structured in a peer to peer fashion. A schema-based peer to peer network such as this would benefit greatly from semantic routing.

Semantic routing techniques uses prospective nodes selected because of another node's confidence in their ability to respond correctly to a given query irrespective of their position within the network. Each time a node answers a query its peers adjust their confidence in that node with regard to that type of query.

The nature of this adjustment depends upon whether the node answered correctly i.e. if the search result was selected by the searcher. The information associated with 'types' depends greatly on the kind of semantic data being dealt with by the network and the strictness of the peer confidence ranking algorithm.. Nodes must have a constant identifier within the network's namespace if they are to retain their confidence ratings.

There is an initial forming stage where none of the peers have ratings for any nodes, and nodes might be returned randomly. It has been observed [25] that a certain amount of random responses to all requests can avoid an effect called 'overfitting', which is when the confidence data associated with the nodes becomes too rigid and inflexible.

Semantic routing is a reasonably new routing technique. The advent of semantic networking is making this an important emerging networking area and one that is sure to grow and flourish in future.

A. *Benefits of Semantic Routing*

1. Scalability: A measure of how a system performs when the number of nodes and/or number of messages on the network grows where semantic routing can be of beneficial in scalability.
2. *Complexity:* the order of steps required for a packet to travel from one host to another in a worst case scenario where semantic can apply in complexity of the packets and host management.
3. *Anonymity:* If a network is to be designed to provide anonymity semantic routing level is a requirement

B. *Application of semantic routing:*

1. *Resource Description Framework***:** is a standard model for data interchange on the Web. RDF has features that facilitate data merging even if the underlying schemas differ, and it specifically supports the evolution of schemas over time without requiring all the data consumers to be changed The view is the easiest possible mental model for RDF and is often used in easy-to-understand visual explanation by implementing semantic routing.
2. *NeuroGrid*: Provide a framework such that entities can be found within a distributed environment. NeuroGrid tries to provide a more general semantic framework within which search can be conducted NeuroGrid nodes maintain a list about which queries other nodes have been good at answering in the past. This allows a NeuroGrid node, when queried about something, to pass back a list of other nodes that could be queried, along with potential answers to the query utilizing semantic routing
3. *Super-peer based networks***:** provide better scalability than broadcast based networks, and do provide perfect support for inhomogeneous schema-based networks,

which support different metadata schemas and ontologies by use of semantic routing.

Semantic routing will be fully implemented especially for future networking technologies since communication is becoming more dynamic and routing of packets through the nodes is very essential. Semantic routing will be one as one of the emerging networking technologies will be fully utilized in to accommodate future adaption and meet user and business needs in term of efficient and reliable communication and delivery.

IX. CROSS-LAYER DESIGN AND OPTIMIZATION

Cross-layer optimization is mode of virtually strict boundaries between layers. The cross layer approach transports feedback dynamically via the layer boundaries to enable the compensation for e.g. overload, latency or other mismatch of requirements and resources by any control input to another layer but that layer directly affected by the detected deficiency.

Cross-layer design and optimization is used to design and improve the performance in both wireless and wired line networks. The central idea of cross-layer design is to optimize the control and exchange of information over two or more layers to achieve significant performance improvements by exploiting the interactions between various protocol layers.

Cross-layer optimization contributes to an improvement of quality of services under various operational conditions. Such adaptive quality of service management is currently subject of various patent applications.

The cross-layer control mechanism provides a feedback on concurrent quality information for the adaptive setting of control parameters. The control scheme applies, the observed quality parameters, logic based reasoning about applying the appropriate control strategy and the statistically computed control input to parameter settings and mode switches.

A. Benefits of Cross Layer and Optimization

Resource efficiency: The control adjusted to availability of limited resources is the first mandatory step to achieve at least a minimum level of quality. Communications system that allows this kind of Cross-layer optimization provides high-speed local area networking over existing power lines, phone lines and coaxial cables. The cross layer design and optimization approach to network stack design is historically a big shift in how one designs communication system. The applications, protocols and hardware need to be re-implemented to be able to support the new extensions and technologies

B. Application

To fully optimize wireless and sensor networks, both the challenges from the physical medium and the QoS-demands from the applications have to be taken into account. Rate, power and coding at the physical layer can be adapted to meet the requirements of the applications given the current channel and network conditions. Knowledge has to be shared between all layers to obtain the highest possible adaptively

The main idea behind cross layer design is to combine the resources available in the different communities, and create a network which can be adoptive and Quality of Service efficient by sharing state information between different processes or modules in the system. Some of the cross –layer design and optimization application includes:

1. *Layer Triggers:* Predefined signals, which are used to notify special events between protocols. The Explicit Congestion Notification (ECN) bit is example of layer trigger. Triggers are cheap and quick to implement, quantifiable performance improvements and compatibility by extending on the strict layered structure. Layer triggers are today extensively used in both wired and wireless networks [16].
2. *MobileMan*: The primary design goal was to implement a system-wide cross layer design in a MANET protocol stack using 802.11. Protocols belonging to different layers can co-operate by sharing network status, while still maintaining the layer separation in the protocol design. Main advantages of their reference design are full compatibility with existing standards as it does not modify each layer' score function, robust upgrade environment and Maintaining the benefits of a modular architecture Aims is to optimize overall network performance, by increasing local interaction among protocols, decreasing remote communications, and consequently saving network bandwidth.
3. *Designing a Mobile Broadband Wireless Access Network:* Designing a Mobile Broadband Wireless Access Network**:** Cross layer design and optimization main design goals is the physical, Medium Access Control and Logical Link layer are jointly optimized, while maintaining the compatibility with the standard IP network architecture. The scheduler in the system becomes the focal point for achieving cross design layer and optimization. Function of any scheduler, intelligent allocation available resources between different users having different QoS demands. Through cross layer design and optimization the scheduler is provided with a rich set of cross-layered information such as traffic packet queue state, QoS demands and channel condition for all users, enabling it to make the best possible decision.
4. *Wireless Sensor Networks (WSNs***)**: Wireless Sensor Networks (WSNs): Goal of any sensor network is to collect and aggregate meaningful information from raw local data obtained by the individual sensor nodes. The number of sensors nodes in a sensor network, combined with the unique characteristics of their operating environment, makes designing WSNs and their applications unique challenges to every researcher/designer.

   Every sensor node reports back to a local hub node within a certain deadline, and since all layers of the protocol [19] stack contributes to energy consumption and delay, an efficient WSN requires a cross layer design across all these layers as well as the underlying hardware [17].

   In conclusion for very task specific purposes a revolutionary cross layer design is often beneficial. By removing every redundant part of the layered structure and the protocols used, there is a highly optimized and power efficient system designed exclusively to be applied to a specific problem.

Indeed this network technology is essential for adaption and utilization of network resources both for users and organization to meet their communication and transmission needs. Cross- layer design and optimization network technology will be fully utilized for existing and future adaption network technologies.

X. CONCLUSIONS

Where almost all aspects of life rely on electronic equipment, the subject of the integrity, secure and satisfaction to end users seems to be crucial for maintaining trust and confidence in the infrastructure and in the digital economy which need regular innovations, research and development with due to emerging networks technologies which addresses the challenges in existence and in future. There are significant opportunities to define new models, mechanisms and techniques addressing multiple areas of the network technologies.

XI. REFERENCES

[1.] P Mell, T Grance, The *NIST Definition of Cloud Computing*, Version 15,1009 Available on: http://csrc.nist.gov/groups/SNS/cloud computing

[2.] D Nurmi, R Wolski, C Grzegorczyk, G Obertelli, S Soman, L Youseff, D Zagorodnov, *The Eucalyptus Open-sourceCloud-computing System*, Proceedings of the 9th IEEE/ACM International Symposium on Cluster Computing and Grid, IEEExplore, visited on 15th August 2009.

[3.] C Hutchinson, J Ward, K Castilon, *Navigating the Next-Generation Application Architecture*, IT Pro, IEEE Computer Society, 2009, March/April 2009, pp 18-22

[4.] Sedayao, Implementing and Operating an Internet Scale Distributed Application using Services Oriented Architecture Principles and Cloud Computing Infrastructure, Proceedings of the iiWAS 2008, November, 2008, Linz, Austria, pp 417-421.

[5.] F Majorczyk, E Totel, L Mé, A Saïdane, Anomaly Detection with Diagnosis in Diversified Systems using Information Flow Graphs, IFIP International Federation for Information Processing, LNCS, Vol 278, pp 301-315, Springer Boston, 2008.

[6.] D Hervé, M Dacier, A Wespi, Towards a taxonomy of intrusion-detection systems, Computer Networks: The International Journal of Computer and Telecommunications Networking, Vol 9, April 1999, pp 805-822.

[7.] C Dimitrakakis, A Mitrokotsa, Statistical Decision Making for Authentication and Intrusion Detection,Proceedings of the 8th IEEE International Conference on Machine Learning and Applications (ICMLA 2009), IEEE Press, December 2009

[8.] M Barreno, B Nelson, R Sears, AD Joseph, JD Tyger, Can Machine Learning Be Secure?, Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS'06), 21-24 March 2006, Taipei, Taiwan

[9.] A Mitrokotsa, C Dimitrakakis, C Douligeris, Intrusion Detection Using Cost-Sensitive Classification,Proceedings of the 3rd European Conference on Computer Network Defence (EC2ND 2007), LNEE (LectureNotes in Electrical Engineering), pp 35-46, Heraklion, Crete, Greece, 4-5 October 2007, Springer-Verlag

[10.] W Fan, W Lee, S J Stolfo, M Miller, A Multiple Model Cost-Sensitive Approach for Intrusion Detection,Proceedings of the 11th European Conference on Machine Learning 2000 (ECML'00), Barcelona, Catalonia,Spain, Lecture Notes in Computer Science, Vol 1810, pp 142-153

[11.] P Pietraszek, Using Adaptive Alert Classification to Reduce False Positives in Intrusion Detection, Proceedingsof Recent Advances in Intrusion Detection 7th International Symposium (RAID'04), Sophia, Antipolis, France, Lecture Notes in Computer Science 3224, Springer, pp 102-124

[12.] E. Hossain, editor (2008). Heterogeneous Wireless Access Networks: Architectures and Protocols. Springer

[13.] E. H. Ong and J. Y. Khan (2010). On optimal network selection in a dynamic multi- RAT environment. IEEE Communications Letters, 14(3):217-219.

[14.] F. H. P. Fitzek and M. D. Katz, editors (2007). Cognitive Wireless Networks: Concepts, Methodologies and Visions Inspiring the Age of Enlightenment of Wireless Communications. Springer.

[15.] F Valeur, G Vigna, C Kruegel, A Kemmerer, A Comprehensive Approach to Intrusion Detection Alert Correlation, IEEE Transactions on Dependable and Secure Computing, Vol 1, No 3, July 2004, pp 146-169

[16.] S. Kunniyur and R. Srikant, \End-to-end congestion control: Utility functions,random losses and ecn marks," Proc. IEEE INFOCOM, vol. 3,pp. 1323{1332, Mar. 2000.

[17.] M. Conti, G. Maselli, and G. Turi, \Cross-layering in a mobile ad hocnetwork design," IEEE Comp. Soc., pp. 48{51, Feb. 2004. Commersial implementation.

[18.] A. J. Goldsmith and S. B. Wicker, \Design challenges for energy-contrained ad hoc wireless networks," IEEE Wireless Communications, pp. 8{27, Aug.
2002.

[19.] http://www.wifinotes.com/how-wireless-sensor-networks-works.html

[20.] http://arni.epfl.ch/contents/courses/monoII.pdf

[21.] http://searchnetworking.techtarget.com/definition/network-coding

[22.] http://www.networkcomputing.com/data-networking-management/229500346

[23.] http://www.articlesbase.com/college-and-university-articles/essay-semantic-routing-4982276.html

[24.] http://electronicdesign.com/article/communications/How-Flow-Processing-Improves-Network-Communications.aspx

[25.] http://www.w3.org/RDF/