Generations and Revolutions of the Infrastructures for Community Network

Avijit Datta

Cooch Behar Panchanan Barma University, India

Abstract
The contents of community network are now-a-days digitally delivered through some electronic channel especially internet. The sharing of multi-media contents digitally is the most concerned of community network research. The community network infrastructure may involve licensed mobile network, internet service provider, internet carriers, internet exchange point, public network operator etc. Several operative model are developed and models differs in the functional parts of different layers and impose several rights like access, withdrawal, management, exclusion and alienation. In the decentralized system, such as peer-to-peer (P2P), the sharing of contents through the community network need to be secured and trust worthy. Quality of Service (QoS) and Quality of Experience (QoE) are the demands of infrastructures for Community Network to minimize the vulnerability of it and maintaining the network protection and robustness are the concern of infrastructures for community network.

Keywords: Generations of Community network, security of infrastructures for community network, P2P content delivery, digital data sharing.

1. INTRODUCTION

A thorough research on challenges related to content delivery for community network has been done by the European Network-of-Excellence CONTENT [1]. In the community network, end-users are not only receiving the contents from the community, they are also producing contents and core elements of the network. So, the delivery is not only limited to the infrastructure path provided by the ISPs.

In [2] the community network is defined as a group of people whose collaboration and communication over network strengthens their shared identity and goal. So, community is not only for collaboration, whereas people are contributing in the community by their resources.

The content delivery is initially done within the community through physical network, without any involvement of internet and not leaving any trace of type of content in the network. This is one of the huge threats to the actual community network connected through the internet. So, the security and vulnerability of the architectural framework related to the content delivery for the community network is the concern and challenge.

The residential internet uses and sharing tends to raise concern about legal issues in Europe. The “FON” (http://www.fon.com) community, which is using Wireless Community Network (WCN) [6] became very popular where the internet is shared using home xDSL and continuing this business illegally. On the other hand, some of the Italian community [3] provides dynamic DNS and PBX service to the members. In India, community members using the network to share file, backup, playback, VoIP along with the internet access of the network.

2. NETWORK ARCHITECTURE & TECHNOLOGY

The community network architecture is depicted in the Fig. 1. which clearly shows that the community network plays the central role to provide communication. It works as content service provider to the local community. For the most community members, it is a fact that the technical concept of the physical (PL), data link (DLL) and the network layer (NL) is minimum. Especially, the DLL, which gives the logical connection within the network using Medium Access Control (MAC) and Logical Link Control (LLC). These helps to establish connectivity using Ethernet with the ISP and handles error correction within the network.

Data link layer attempts to provide reliable communication over the physical layer interface. It breaks the outgoing data into frames and reassemble the received frames. It helps to create and detect frame boundaries. Handle errors by implementing an acknowledgement and retransmission scheme. Implement flow control [4]. It supports points-to-point as well as broadcast communication. It also supports simplex, half-duplex or full-duplex communication.

Implements routing of frames (packets) through the network done at network layer. It defines the most optimum path the packet should take from the source to the destination. It defines logical addressing so that any endpoint can be identified [5]. It handles congestion in the network. Facilitates interconnection between heterogeneous networks (Internetworking). The network layer also defines how to fragment a packet into smaller packets to accommodate different media.

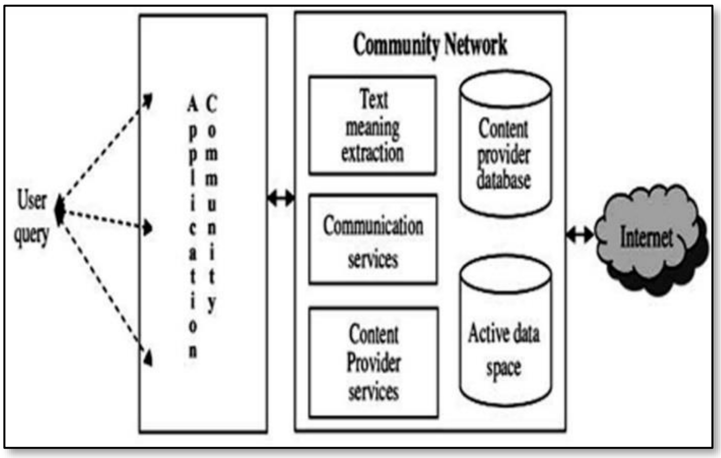

Figure. 1. Architecture Framework

The community network is the combination of several network technologies such as mobile IPv4 and IPv6, network mobility (NEMO), mobile ad-hoc network (MANET), wireless mesh network (WMN), wireless sensor network (WSN) etc. So, the management and configurations of these technologies are concern and left challenging research environment. The community requires handover process of technologies within the so called network like Figure. 2. (Media-Independent Handover Tutorial, 2006) [7]

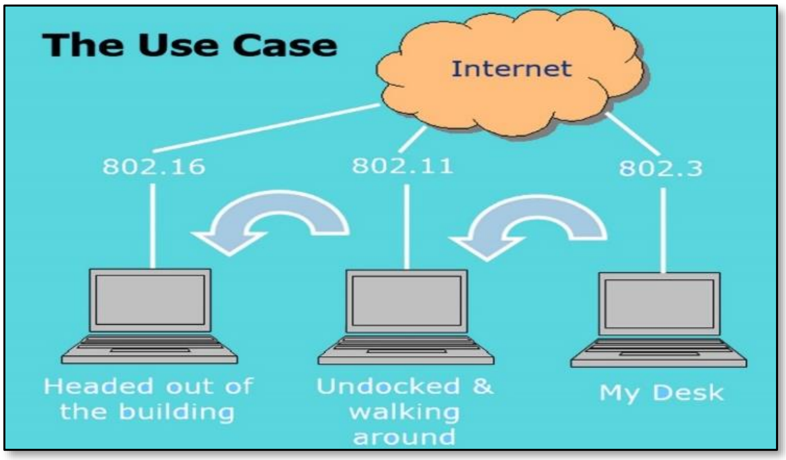

Figure. 2. Technology handover

The hand over process can easily been derived with IEEE 802.3 (Ethernet) to 802.11 (WLAN) to 802.16 (WMAN). These three standards of IEEE combined to 802.21 (Media Independent Handover Services) and deals with heterogeneous network types. The functioning of 802.21 is as in Figure. 3. (Media-Independent Handover Tutorial, 2006) [7]

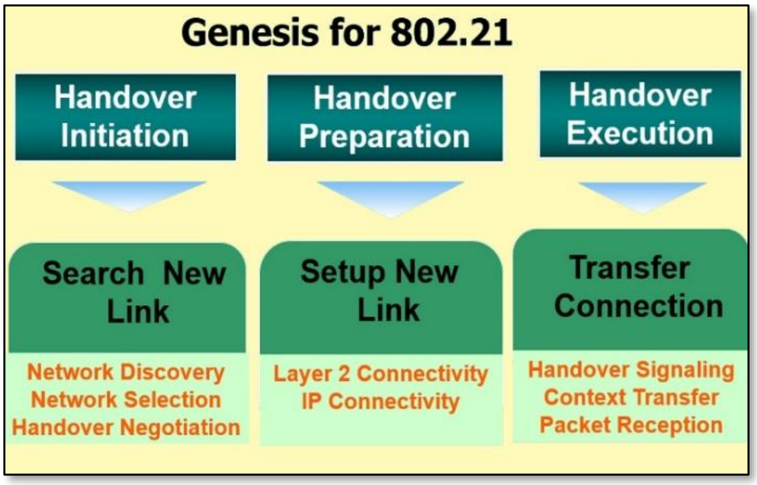

Figure. 3. Genesis of 802.21

For the multimedia transmission, the handover execution section of Figure. 3. should maintain the QoS because the multimedia transmission is always a real-time delivery.

3. GENERATIONS OF TECHNOLOGY

The Figure. 2. Clearly shows the technologies are involved in the community network. The technologies are changing, in due course, with different levels of users (members) involved in the network. Moreover, the type of technology involvement may depend upon the type of data sharing between the members too.

3.1 ETHERNET: 802.3

The IEEE 802.3 or Ethernet standard is used to establish network connection between and within the physical layer of members of the community network and the external internet connectivity. The Ethernet is to prepare data into frame format as shown in Figure. 4.

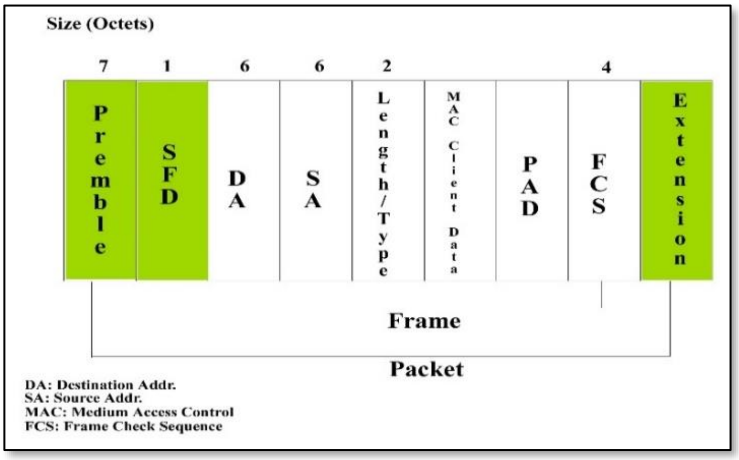

Figure. 4. Layout of Ethernet 802.3

The communication using Ethernet is there to set bandwidth for data transmission through the media between the members of the network. The Data Link Layer of OSI model is involved to hold connection with MAC Control and MAC. The data transmission 1 Mb/s to 10 Mb/s, the Physical Layer Signaling (PLS) required between MAC and Physical Medium Attachment (PMA) using Attachment Unit Interface (AUI), Medium Attachment Unit (MAU) and Media Dependent Interface (MDI). With these combinations, Ethernet transmit the data content to the higher layers with the help of Logical Link Control and MAC Client.

There will be some technical changes require to achieve bandwidth 100 Mb/s and above. There will be Reconciliation Sublayer (RS) between MAC Control and Physical Layer Device using different types of Medium Independent Interface (xMII) and MDI. The block diagram is showed in Figure. 5.

The original intention of Ethernet was never to use its data link layer as the means for providing guaranteed delivery of data. It was always the intent that a higher layer protocol would do that service. Therefore, it was only necessary to identify by number which higher layer protocol was being used through the two-byte field in the DIX frame. Originally, Xerox maintained the assignments and now IEEE provides the administration.

The 802.3 standard does not include the type field but instead defines it as a length field. Per the 802.3 standard, a value in this field of 1518 or less indicates the length of the data field, while values above this may be ignored, discarded or used in a private manner. These out of bound values could then be used to identify higher layer protocols just like DIX frames [17].

Although Ethernet was originally designed as a coaxial bus system, alternate physical layers have evolved since the early 80s. The IEEE 802 committee has defined several physical layers and that is why it is important to specify the correct option when selecting Ethernet.

What has been discussed is the operation of Ethernet’s physical and data link layers. This alone does not implement an industrial communication network. What is needed is transport layer for reliable transfers of messages and an application layer which provides the actual control commands and responses.

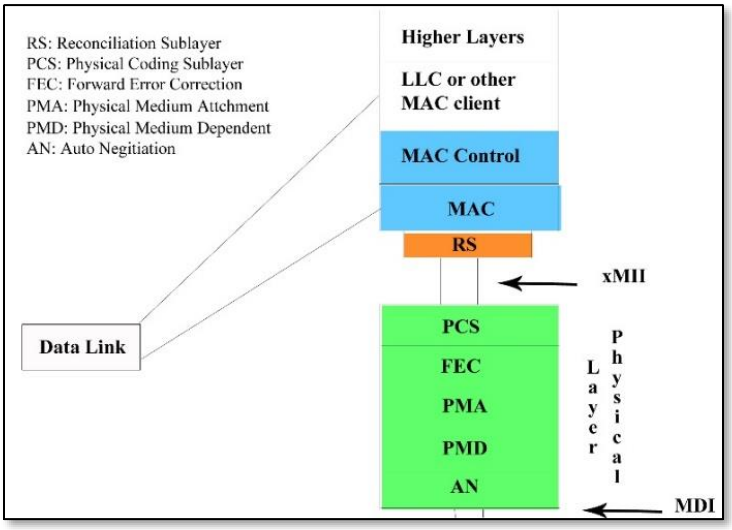
RS: Reconciliation Sublayer
PCS: Physical Coding Sublayer
FEC: Forward Error Correction
PMA: Physical Medium Attchment
PMD: Physical Medium Dependent
AN: Auto Negitiation
Higher Layers
LLC or other MAC client
MAC Control
MAC
RS
xMII
Data Link
PCS
FEC
PMA
PMD
AN
Layer
Physical
MDI

Figure. 5. Block Diagram for 802.3 of 100 Mb/s and above

The Ethernet is fulfilling the demand for increased bandwidth between connected devices, bridging of data centres and bridging of audio and video with the emerging technologies.

The core networking of Ethernet is dealing with more user with more bandwidth and application covering large area, ISPs, xDSLs, YouTube, Facebook, Netflix etc.

3.2 WIRELESS LAN: 802.11

Wireless LAN, 802.11, uses common MAC to all physical layer standards. The physical layer of 802.11 is split into two sublayers as Physical Layer Convergence Procedure (PLCP) and Physical Medium Dependent (PMD).

The MAC layer of 802.11 provides two different services to exchange data packets, broadcasting, multicasting and exchange of bounded delay using mandatory Asynchronous Data Service and optional Time Bounded Service. It helps to avoid collision by sending ACK packet for acknowledgement. It also put virtual carrier sensing and utilize access points terminal as per list.

The infrastructure of 802.11 is similar to the architecture of cellular network. The network stations (STA) are consists of terminal with access mechanism in wireless mode to communicate integrated stations in the wireless LAN called access points (AP). A group of terminals as basic service set (BSS) are using same set of APs. A Distribution System is there in between the different BSS and wired points. The Figure. 6 (IEEE 802.11 Standard (WLAN) Tutorial) [9] is given below to depict the infrastructure of 802.11 with clear vision.

The 802.11 WLAN is currently having a great momentum in use. Industries from small to large scale, retailers, hospitals, airports, railways all are using and providing wifi facilities. It may lead to network security attacks. The attacker may use the active or passive attack concept [14].

Active attack may be of following ways:

- Masquerading.
- Replay.
- Authentication spoofing.
- Message injection.
- Man in a Middle Attack.
- Message Modification.
- Denial-of-service.

- Message Decryption.

Passive attack may be of following ways:

- Eavesdropping.
- Dictionary based attack.
- Traffic Analysis.
- Cracking the WEP key.

The security of WLAN may be maintained by using:

- Data confidentiality and integrity.
- Authentication and access control.
- Intrusion detection and prevention.
- Broader security consideration.

The authentication may Open System authentication or Shared System authentication. The WLAN administrator may have the option to send unencrypted packets and allow air encryption [15]. To control the vulnerability of 802.11 can be managed by some steps aid process:

- Establishing security policy for WLAN.
- Security design.
- Logical separation of internal network.
- Enabling VPN connection only.
- Restricting Access Points.
- Restriction on protocols.

The installation location of APs is another security issue because of placing APs inappropriately will expose it to physical attacks. Attackers can easily reset the APs once found causing the AP to switch to its default settings which is totally insecure. It is very important for network security administrators to carefully choose appropriate places to mount APs.

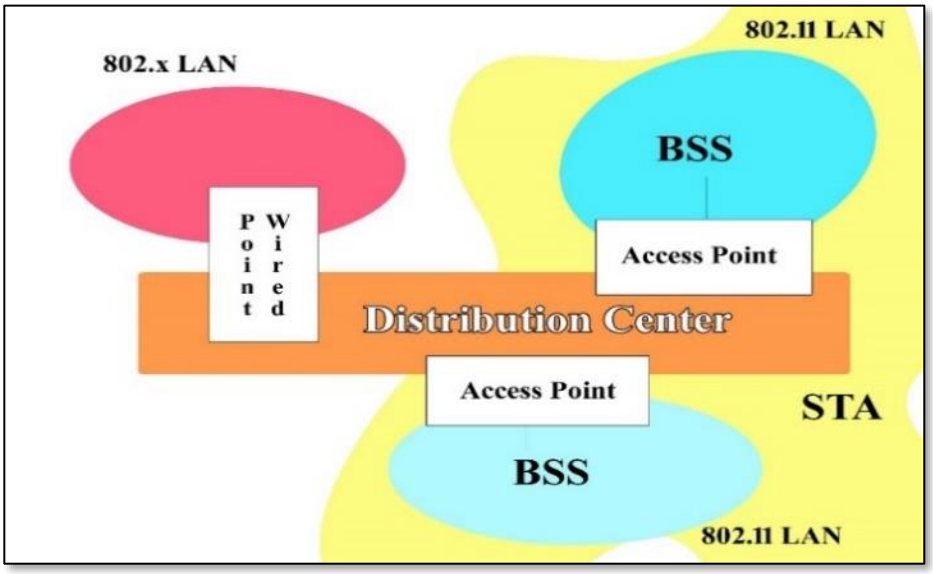

Figure. 6. Infrastructure of 802.11

There are different protocol versions of 802.11 for different frequency and bandwidth like 802.11a, 802.11b, 802.11g and 802.11n with bandwidth ranging from 6.5 Mb/s to 200 Mb/s.

The main ideas of MAC of 802.11 is CSMA/CA strategy i.e. CSMA protocol with collision avoidance feature. It does inter frame spacing and medium access. Each frame is associated with retry counter depending upon the frame size and fragments are given a maximum lifetime by MAC before it is being discarded.

The main problems with the 802.11 or WLAN problems are hidden terminal and exposed terminal problem. So that the Aps are managed with authentication and association by shared key within the community members of the BSS. To guaranteeing the desired QoS, 802.11e proposes an enhanced MAC protocol which includes new traffic categories.

The security solution, by 802.11, will be provided by confidentiality, authentication and integrity and maintain reasonable processing.

3.3 WIRELESS MAN: 802.16

IEEE Standard 802.16, with its Wireless MAN air interface standard for fixed wireless metropolitan area networks operating anywhere in the world in appropriate licensed or license-exempt spectrum between 2 and 66 GHz. The technology is designed to support multiple services simultaneously and so is capable of providing an area’s primary infrastructure for data, voice, and other services, in both residential and commercial applications [10].

The design of MAC protocol for 802.16 has been changed to time division multiplexing/time division multiple access (TDM/TDMA) protocol. The new protocol technology supports time division duplexing (TDD), frequency division duplexing (FDD) and half-duplex frequency division duplexing (H-FDD) [11]. The physical layer (PHY) transmission block diagram of 802.16 is shown in Figure. 7:

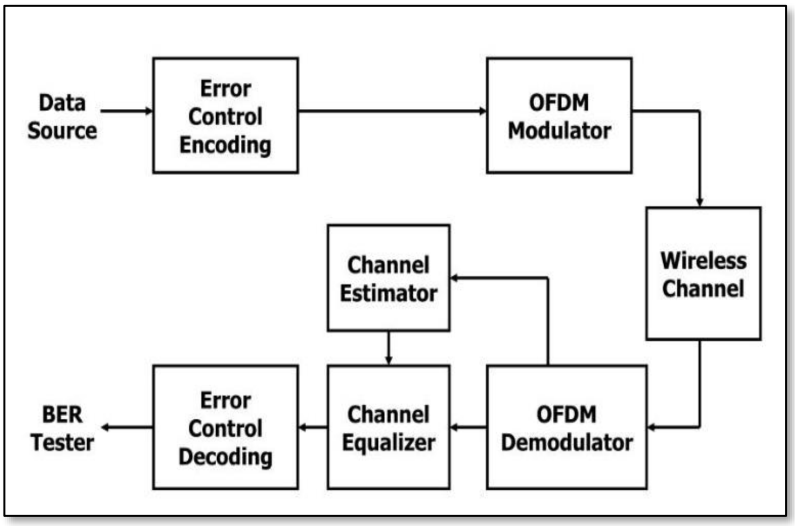

Figure. 7. Block diagram for PHY of 802.16

The 802.16 working group involves two activities:

- Project P802.16-REVd: Technical enhancement with three air interface standards and adding 2-11 GHz. specification.
- Project P802.16e: Support for mobile users.

The main reasons behind the deployment of 802.16 is

- To fulfill the lack of significant broadband infrastructure.
- To provide multi-service network like advanced real-time services.

- Location flexible and cost efficient.
- It supports wireless LAN access point as per need.
- Deployment in geographically large area.

The IEEE 802.16 Working Group is to Broadband Wireless Access anticipating the world's need for broadband wireless metropolitan area networks. It has completed a set of standards that are currently moving innovative technology into the broadband access marketplace. A wide range of applications is anticipated [10].

4. MEDIA INDEPENDENT HANDOVER

Media Independent Handover, the IEEE 802.21 standard is an 802 standard for technology handover service. The needs for the handover service are:

- Wrong selection of network from the available APs.
- Multiple interfaces on devices.
- Construction of media independent form.

Community members are keen to cellular interworking using wired and wireless platform. They are readily using 802.11 and 802.16 and need to handover technologies independently.

In the multi-radio networking evaluation, it is need of multiple wireless technologies with more capable devices like mobile, tab etc. and various evolving usages of model network.

The handover of technology, for the infrastructure of community network, is of two broad type. The horizontal or homogeneous handovers works with localized mobility i.e. within the single network with limited opportunity. The other is vertical or heterogeneous handovers with globally different network with more opportunity. The 802.21 is not only for handover initiation but also to select network and activation of interfaces. The handover standard is shown in Figure. 8.

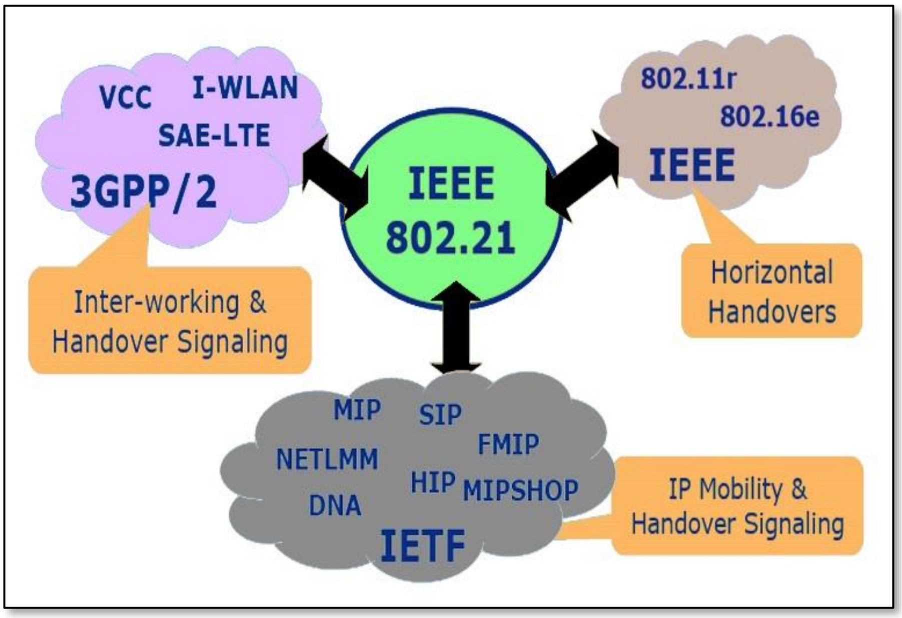

Figure. 8. Handover Standards

The Media Independent Handover included services like optimizing the layer 3 and above handovers. The handover extends to cellular network from 802.3 to 802.11 to 802.16. It also provides service for seamless roaming to maintain connection and low power operation for multi-radio devices. The key services and technology handovers of the 802.21 is given in the Figure. 9 (Media-Independent Handover Tutorial, 2006) [7].

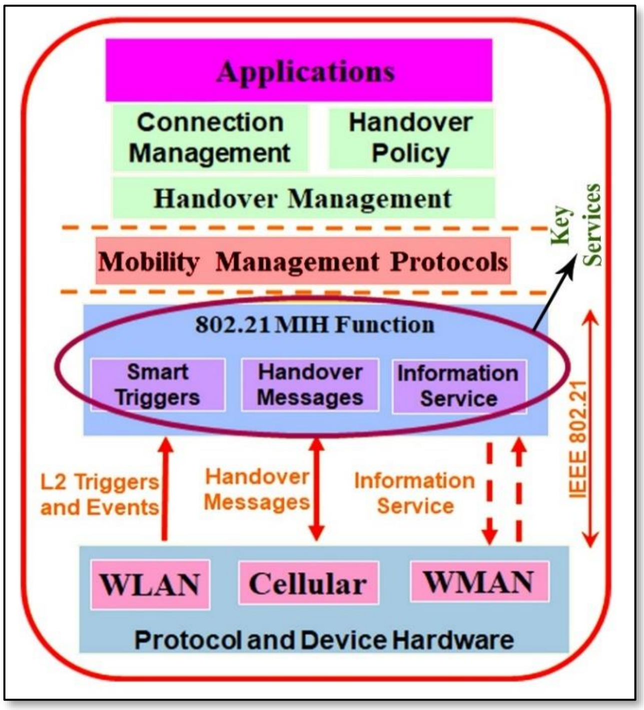

Figure. 9. Key Services and Technology Handovers

802.21 information server holds the list of available networks like 802.11/16/22, GSM, UTMS, information of link layers with neighbor maps and higher layer services like ISP, MMS etc. Information of all available network is also means to indicate the presence of WiFi hotspots [16].

The 802.21 maintains network access security by using network access authentication, secure association and access control with ciphering. To maintain the security, the entities that are involved are:

- Mobile node.
- Access point for point to point attachment.
- Authentication server.

The mobile node changes its point of attachment due to handover only. The network access security is all about how to use the three steps together to get perfect security for the network and its members with the use of security association.

Link-layer data frames are cryptographically protected with the use of ciphering keys depending on underlying link-layer technologies (Media-Independent Handover Security Tutorial, 2008) [8]. The two common handover scenarios may be intra-technology and inter-technology handovers.

The intra-technology handovers like AP to AP, BS to BS, typically within the same domain. The inter-technology handover may be dual and single radio handovers. The handovers within same domain and different domain has different challenges.

5. MOBILITY NETWORK MODELS

T. Camp, J. Boleng, and V. Davies in [12] described the group mobility models for community network. These models may help a mobility network to take decision to move forward to any other group of mobility network. Mobility network models may be type of:

- Exponential Correlated Random Mobility Model.

- Column Mobility Model.
- Nomadic Community Mobility Model.
- Pursue Mobility Model.
- Reference Point Group Mobility Model.

The mobile network uses both IPv4 and IPv6 versions of Internet Protocol (IP). For the mobility network it is essential to keeping fixed IP for individual instruments as Home Address. So, handover from IPv6 to IPv4 as First Handover [13] or other types improved handovers may require. The mobility network models with handovers may require the following software and hardware.

- Access Point (AP) / Router.
- Mobile Node.
- Home Agent.
- Corresponding Node.

Passive and active handover measurement can be done for the mobility network handovers.

6. DISCUSSION AND CONCLUSION

The network infrastructure provides connectivity along with critical resource for the digital data sharing and becoming important for the social inclusion and public platform participation [18]. For the internet connectivity, there are several technical and operational ways and network infrastructures are developed as common property and maintained by common resource principles. In the community network, there must have a provision to create individual connectivity by their own and there are many examples of self-organized network for community networking [19].

The internet is the most important resource and internet cannot work without suitable network infrastructure and relevant content and services. For any network to start, it requires at least network infrastructure that provides the connectivity. The basics that routers and links are require for development and exchange of contents and services.

A critical feature of network infrastructure commons is the potential for members of community: the idea that anyone can expand the network. Contributing to network infrastructures creates social and economic benefits for everyone. Therefore, these public interest activities should be increased, and should be with tax deductions. These deductions policy available in many countries, although accessing them requires legal knowledge and organisational structure.

With advances in devices and networks multi-layer community models are likely to become norms. Sharing of bandwidth with proper identification of the terminal and their authentication, for the security of the data transmission within the community network is very much essential.

It is visible that their technology and protocol changes take place while communication establish between the terminals. So security of any aspect should not be compromised.

802.21 helps with technology handover initiation, network selection and interface activation during the vertical handover. It also enables co-operative handover decision making between client and network. So the media independent handover has a huge impact on the infrastructure of community network and becoming popular for that.

REFERENCES

1. Plagemann T., Canonico R., Domingo-Pascual J., Guerrero C., Mauthe A. (2008) Infrastructures for Community Networks. *Content Delivery Networks. Lecture Notes Electrical Engineering*, vol 9.

Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-77887-5_15.

2. Rosson MB., Carroll JM. (1998), Network communities, community networks. *CHI 98 conference summary on Human factors in computing systems*, pp. 121–122, https://doi.org/10.1145/286498.286568.
3. Lum WY., Lau FCM. (2002) A context-aware decision engine for content adaptation. *IEEE Pervasive Computing*, 1(3):41–49.
4. Akyildiz IF., Wang X., Wang W. (2005) Wireless mesh networks: a survey. *Computer Networks*, Vol. 47, no. 4, pp. 445–487, DOI: 10.1016/j.comnet.2004.12.001.
5. Biswas S., Morris R. (2005) Opportunistic Routing in Multi-Hop Wireless Networks. *Proceedings of SIGCOMM 2005*, Philadelphia, PA, USA, pp. 69–74.
6. Venkatesh M. (2003). The Community Network Lifecycle: A Framework for Research and Action. *Special Issue: ICTs and Community Networking.* The Information Society, 19, 339 - 347.
7. Media-Independent Handover (IEEE 802.21) Tutorial (2006), https://www.ieee802.org/21/Tutorials/802 21-IEEE-Tutorial.ppt.
8. Media-Independent Handover Security Tutorial (2008) https://www.ieee802.org/21/Tutorials/802 21-IEEE-Security_Tutorial.ppt.
9. IEEE 802.11 Standard (WLAN) Tutorial https://www3.cs.stonybrook.edu/~jgao/CSE370-spring10/80211.pdf.
10. Roger B. Marks (2003). IEEE standard 802.16 for Global Broadband Wireless Access. *National Institute of Standards and Technology (NIST), Boulder, Colorado, USA, Chair, IEEE 802.16 Working Group on Broadband Wireless Access (2003)*. Session: The Future of Wireless.
11. Eklund, et. al. (2011). *IEEE 802.16 standards: The working group and documents*. 10.1002/9781118098875.ch2.
12. Camp, Tracy & Davies, Vanessa. (2002). A Survey of Mobility Models for Ad Hoc Network Research. *Wireless Communications and Mobile Computing 2*. DOI: 10.1002/wcm.72.
13. Cabellos-Aparicio A., Serral-Gracià R., Jakab L., Domingo-Pascual J. (2005). Measurement Based Analysis of the Handover in a WLAN MIPv6 Scenario. *Dovrolis C. (eds) Passive and Active Network Measurement. PAM 2005. Lecture Notes in Computer Science*, vol 3431. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-540-31966-5_16.
14. Leandro Navarro (2018), *Network Infrastructures, The Commons Model for Local Participation, Governance and Sustainability*, APC.
15. Ertaul, Levent & Catambay, Omicel. (2009). Today & Tomorrow: IEEE 802.11 WLAN Security. 73-77.
16. Poderi, Giacomo. (2019). Sustaining platforms as commons: perspectives on participation, infrastructure, and governance. *CoDesign. 15*. 243-255. DOI: 10.1080/15710882.2019.1631351.
17. Porpora, D. V. (1989). Four concepts of social structure. *Journal for the Theory of Social Behavior* 19(2):195–211.
18. Buriyameathagul, K. (2013). Characteristics of Culture in Thai Society and Virtual Communities. Silpakorn University Journal of Social Sciences, Humanities, and Arts, 13(2), 207-270.
19. Brown, J. S., and Duguid, P. (1994). Borderline issues: Social and material aspects of design. *Human-Computer Interaction* 9:3–36.