Tactical Wireless Network and Commercial Wireless Network

Rita Mahajan
Assistant Professor, Electronics and Communication Engineering Department,
Punjab Engineering College (Deemed to be University), Chandigarh, India.

Abstract: In this paper a comparison has been presented between tactical wireless networks and commercial wireless network. The implications of cognitive radio technology have also been explored for upcoming tactical wireless networks, considering benefits, technical aspects and security. Many organizations and nations are planning to apply Cognitive Radio Network technology (CRNT) to tactical wireless communication networks. This study will also describe that why tactical wireless networks have been lag behind than commercial wireless networks in technology. As a result, the military and defense organizations are interested in implementing some latest technologies of commercial network in their own networks without doing any compromise on security aspect.

Keywords: Cognitive radio, tactical networks, wireless networks, Cognitive Radio Network technology.

I. INTRODUCTION

Although military operations were the main motivation for the development of the wireless communication technologies in the beginning but from almost past two decades commercial wireless networks are showing progress at a very high pace as compared to tactical wireless networks. In last twenty years, there is significant progress in commercial wireless communication technology. The number of devices and people connected to internet has significantly increased. Most of the locations have excellent and reliable connectivity with drastically reduced price. People are using the latest technology available and asking for more capabilities to fulfil their requirements. These wireless equipments such as cell phones, smart TVs, laptops tablets etcetera provide us connectivity to the whole world. These devices have become an integral part of our lives.

During the World War I, wireless communication by means of radio frequency signal was used by military for the first time. Telegraph radios were used for long distance communication. These radios were installed in airplane for pilot to communicate with headquarter at ground. At that time the wireless technology was not advanced and reliable, so it was not very attractive for defense department. It became attractive during World War II for voice communication. During that time, wireless communication technologies were using analog signals for broadcasting and for point-to-point communication.

Now all wireless communication technologies are based on digital signals and lot of data can be transmitted at very high speed. The requirement of data to be transmitted via wireless channel is increasing day by day in commercial as well as tactical networks. In military operations, position of the troops and data of various sensors need to be shared between military units. Wired network is still required as a backbone along with the wireless communication network. Conventional wireless communication networks are discussed in section II and tactical wireless network are discussed in section III.

II. Conventional Wireless System

In this section the broad architecture of conventional wireless communication networks has been discussed. Modern commercial wireless communication system is very successful in creating superb coverage with very high reliability. Moreover it can be afforded by most of the people. All cellular phone users (mobile end users) are connected to the base stations by the service providers. The towers of base stations are part of a fixed network and are connected to a base station controller (BSC). All base station controllers are connected to a core network via gateway. Functioning of conventional wireless network is discussed here in brief. Third Generation Partnership Project which is collaboration between groups of standardization committees for telecommunication, have established some regulations for various mobile technologies such as GSM, 2G, 3G, 4G and LTE etc. The significant aspect of this project is defining the standard 'Interface Control Documents' (ICDs) for all interfaces. Document for end user to base station air interface is called ICD I, base station to base station controller is called ICD II and ICD III defines the interface between core network to base station controller. So four entities, known as end user, BS, BSC and Core network need three open standard 'Interface Control Documents' to function properly. The block diagram of conventional system is shown in Fig. 1. Other ICDs have been defined for handover of end users between different base stations.

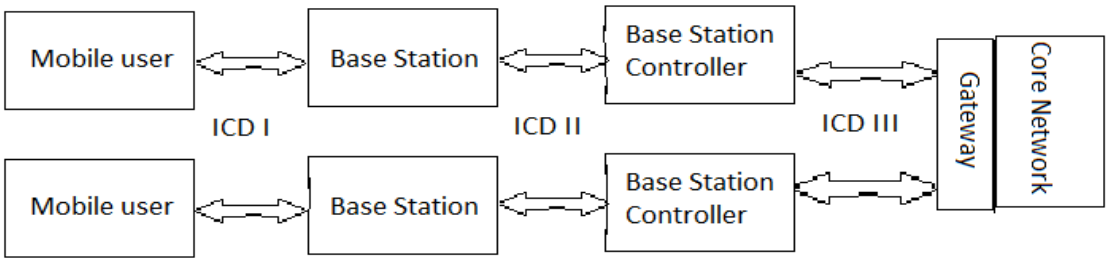

Figure 1: Entities and ICDs for conventional wireless network

Following are the advantages of the properly defined entities and their interfaces for architecture of network.

Standardization: The manufacturers of technologies need not to worry about designing interfaces. All the interfaces have been predefined by open standard 'Interface Control Documents'. They (vendors) just have to work for designing the entities (user equipment, Base Station, Base Station Controller, gateway, and core network etc.)

Healthy competition: Service providers need to buy all entities from vendors to install and setup a network. They can explore the market for better price and quality. All entities can be bought from different vendors due to standardization and a healthy competition is created among vendors. As a result cost decreases and quality improves. Moreover some vendors can plan to manufacture only one entity which further reduces the cost.

Modernization: All manufacturers of these entities are putting great effort to make their product most compact and provide better quality of service.

For commercial wireless network, number of users is in millions. This can motivate the vendors to invest in research and development centers of their own. On the contrary, in tactical networks, the market size is very small. All the developments done for commercial wireless communication model cannot be used as such in tactical wireless networks.

III. Tactical Wireless Network

When a wireless communication network is used to help the operations of military and defence services then it is called tactical wireless network. It consists of some special features that are different from commercially available wireless network. The main characteristic of tactical wireless network is that it should be able to function under aggressive conditions. It must be able to operate in rough and tough environment. This rough and tough environment consists of attacks from the forces of enemies, interferences from the neighbouring networks, and mobility of armed force. All these factors of the environment add lots of unreliability to the operation of tactical wireless networks. Tactical wireless networks are also improving but at a modest rate resulted in development of new generation of mobile ad hoc networks (MANETS) and introduction of cognitive radio based tactical wireless networks[1]. The requirements of tactical networks are completely different as compared to commercial wireless networks and these differences are one of the important factors leading to the gap in their development rate. Major differences between commercial wireless networks and tactical wireless networks are discussed one by one below.

a) Infrastructure

Commercial wireless networks rely on deployment of a well-established infrastructure and maintenance which includes continuous monitoring. A commercial wireless network has base stations with fixed network towers. These base stations may collectively be connected to base station controllers and the controllers are connected to core network station through a gateway. The end mobile users get services through fixed network towers and in this way commercial networks have well established hierarchy on fixed locations. In contrast tactical wireless networks are neither having fixed locations for base stations nor an established infrastructure. A dynamic networking model is required in case of tactical wireless networks which should also have capability to tackle with hostile attacks. MANETS [2] are the outcomes of this dynamic requirement of tactical networks.

b) Ad hoc networks

Commercial wireless networks in most of the cases require only one hop network as there is a single wireless link from mobile user to the core hub and these hubs are connected to other hubs or networks through optical fibres or cables whereas in tactical wireless networks single hop networks are not sufficient because multiple wireless links are needed to be established in hostile environment in order to improve range and diversity. One hop ad hoc networks have well developed protocols and architectures and also well-established theoretical models such as Shannon's model and due to which it is very easy to foresee the behaviour and performance of these types of networks. Multi hop ad hoc networks are not having such established wireless models and prediction of performance in case of multi hopping networks is not much authenticate and is prone to errors which makes it difficult to realize tactical wireless networks as compared to commercial wireless networks. Moreover due to dynamic behaviour of tactical networks, it is very difficult to define environment in their prediction model.[3]

c) Bandwidth and intermittent interference

The amount of bandwidth which is required for the proper functioning of the network is sufficiently available in commercial wireless networks but in tactical wireless networks, there is scarcity of bandwidth.[4] Available bandwidth is very limited than the

system specifications. This limitation is due to requirement of bandwidth for security issues, mobility and some other purposes in addition to conventional requirements. Tactical wireless networks are very prone to intermittent interference due to hostile attacks, multipath propagation, dynamic nodes, noise in different terrains may change from hills to forests to plains to seas. All such interferences lead to deterioration of SINR (Signal to interference pus noise ratio) and thus causing loss of information and instability in tactical wireless networks. In comparison, commercial wireless networks are free from most of these interferences as there are no hostile attacks, propagation is single path, terrains are well defined in advance and nodes are static and hence they are more stable and their implementation is easy.

d) Security

Robust and reliable security system is one of the most critical requirements of the tactical wireless networks as these types of networks are always prone to attacks by their adversaries.[5] These security issues include both physical as well as electronic attacks by the enemies. In physical attack, an enemy may directly destroy mobile nodes or may steal some hardware. Electronic attacks are more common these days and needed to be taken care. Electronic attacks may be done with a number of ways. An enemy may send a large number of data packets and thus causing flooding and congestion problems in the network. Rivals may also attack the network by sending jamming signals and disrupting whole communication in the network. The rival may also forge as a regular node in the network and may try to steal confidential information. The forged adversary node may also modify the information and can send wrong information and make the communication unreliable. Due to all the discussed problems, robust security system is the main aspect in tactical wireless networks. Cognitive radios are emerging as a solution for security problem of tactical wireless networks.

e) Competition

Due to lot of competition in commercial world, there are number of service providers and vendors. So a service provider can purchase some base stations from one vendor and more base stations if required from some other vendors.[6] Similarly services of base station controllers and core gateways can be taken from a number of vendors. The service provider can use services and devices from different vendors to build a complete network. Availability of a number of vendors creates competition and reduces the cost for building the network. Building and deploying a tactical network is completely different as deployment of tactical wireless network is done by a single integrator who cannot take any external help and can only go for in house solutions due to security issues. All these results in increase in network building cost.

f) Multiple heterogeneous networks

Homogeneity reduces a number of network designing issues in commercial wireless networks whereas due to need of deployment of heterogeneous networks, tactical wireless networks become very difficult to design.[7] Commercial wireless networks have tendency to work within their prescribed limits and they also have a very good control on all the equipments and services that are available in their network**.** On the other hand, a number of parallel networks such as Soldier Radio Waveform, Wideband Networking Waveform, High band Networking Waveform and Net Centric Waveform are all needed to be deployed in one geographical region in case of tactical wireless networks. Although it is quite difficult to impose such type of heterogeneous networks but after implementation they have several benefits over homogeneous networks. Heterogeneous networks are more robust when compared with homogeneous networks and they can perform well in severe conditions. Also in case of a purposeful attack by the rivals, all the networks can be made to solve different problems and hence leading to the solution in a collective manner.

g) Network Management

Network management is required to control all the operations in wireless network systems. Commercial wireless networks require management of a single network and that too in a static environment whereas tactical wireless networks involve very complex networks and that too in a dynamic environment.[7] The requirement of complex dynamic network management is also an issue because most of the work done till now is on the management of single static networks. Moreover it is very difficult to keep track of the rapid change in network in an unstable and hostile environment for the network management system. Complex networks become easy to achieve if behaviour of network can be predicted but prediction of tactical wireless networks is another difficult task and hence it becomes very difficult of design network management systems in case of tactical networks.

h) Performance

Performance in wireless communication networks is measured in terms of throughput, delay, outage probability and errors in packet transmission.[8] Forward error correction code and automatic repeated request are some techniques which commercially wireless networks are already using to rectify problem of information loss but these techniques do not give good results in tactical networks due to poor network conditions. Adaptive Reed-Solomon codes along with automatic repeated request technique were proposed by Grushevsky and Elmasry for successful message delivery in tactical wireless networks but the solution showed limitation in case of limited bandwidth.[9]

IV. Comparison of tactical and commercial networks

Tactical wireless networks are different from commercial networks in security constraints, anti-jamming needs, mobility of nodes, dynamic topology, deficiency of bandwidth, and other characteristics.

The network is ad hoc (MANET) and it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. The nodes of this network are mobile and end user nodes are the part of infrastructure. Here are some points of comparison of the two networks are given in table 1.

Table 1: Comparison of commercial and tactical wireless network

Parameters	**Commercial network**	**Tactical wireless network**
Infrastructure	Having fixed infrastructure without including end-users in the infrastructure	All nodes are mobile i.e. infrastructure is not fixed, including the end-user nodes.
Network topology	Static backbone network topology	Highly dynamic network topology
Environment and stability	Relatively caring environment and connectivity.	Hostile environment and irregular connectivity.
Network components	Base stations, BS controllers, Core Network	Unmanned aerial vehicle(UAV) , wireless sensor nodes, Information grids
Complexity of devices	Low complexity of mobile devices	Intelligent mobile devices are required
Maintenance	High cost of network maintenance	Maintenance operations are built-in

V. Conclusion

The major challenges for tactical networks have been discussed in this paper. As tactical wireless networks have to deal with a number of issues such as bandwidth scarcity, congestion, security issues and interference, they perform badly as compared to commercial wireless networks as they do not have any of these problems. Tactical networks face highly dynamic environment and lack proper infrastructure. So designing and deployment of efficient, secure and reliable network is the big challenge.

References

[1] Houjeij, A., Saad, W. and Basar, T., 2013, December. Evading eavesdroppers in adversarial cognitive radio networks. In *Global Communications Conference (GLOBECOM), 2013 IEEE* (pp. 611-616).

[2] Burbank, J.L., Chimento, P.F., Haberman, B.K. and Kasch, W.T., 2006. Key challenges of military tactical networking and the elusive promise of MANET technology. *IEEE Communications Magazine*, *44*(11).

[3] Cheng, X., Huang, X. and Du, D.Z. eds., 2013. *Ad hoc wireless networking* (Vol. 14). Springer Science & Business Media.

[4] Suri, N., Benvegnù, E., Tortonesi, M., Stefanelli, C., Kovach, J. and Hanna, J., 2009. Communications middleware for tactical environments: Observations, experiences, and lessons learned. *IEEE Communications Magazine*, *47*(10), (pp 56-63).

[5] Refaei, M.T. and Bush, J., 2014, October. Secure Reliable Group Communication for Tactical Networks. In *Military Communications Conference (MILCOM), 2014 IEEE* (pp. 1195-1200). IEEE.

[6] Elmasry, G.F., 2010. A comparative review of commercial vs. tactical wireless networks. *IEEE Communications Magazine*, *48*(10), (pp 54-59).

[7] Vassiliou, M.S., Agre, J.R., Shah, S. and MacDonald, T., 2013, November. Crucial differences between commercial and military communications technology needs: Why the military still needs its own research. In *Military Communications Conference, MILCOM 2013-2013 IEEE* (pp. 342-347). IEEE.

[8] Pawgasame, W. and Wipusitwarakun, K., 2015, April. Tactical wireless networks: A survey for issues and challenges. In *Defence Technology (ACDT), 2015 Asian Conference on* (pp. 97-102). IEEE.

[9] Grushevsky, Y.L., Elmasry, G.F., Argentieri, S.R. and Lussier, R., 2006, October. Adaptive RS code for message delivery over encrypted military wireless networks. In *Military Communications Conference, 2006. MILCOM 2006. IEEE* (pp. 1-5). IEEE.