International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-12, Special Issue-1, March-2024
https://doi.org/10.55524/CSISTW.2024.12.1.64
Computing for Sustainable Innovation: Shaping Tomorrow's World (CSISTW-2024) on 16th-17th February, 2024
Organized by B.N. College of Engineering and Technology, Lucknow, India

Reducing Packet Delay and Loss in Heterogeneous 5G Mobile Wireless Network

Satya Prakash Adim

Department of Computer Science and Engineering, Institute of Technology and Management, Lucknow, India

Correspondence should be addressed to Satya Prakash Adim; satyaprakashadim@gmail.com

ABSTRACT: Reconstruction and catastrophe response require effective communication. However, the bulk of public safety land mobile radio (LMR) networks now in use only provide narrowband phone service and only partially support low- speed data services due to packet loss, delay, and reduced resource usage. Thus, high resource usage strategies are needed. The Session Initiation Protocol (SIP) and a common radio resource management framework are the technologies now in use to enable interoperability between cellular and LMR networks.SIP stands for Seamless Handoff Protocol. Here, we explore ways to enhance LMR's interoperability with commercial WCNs, which can provide first responders a host of benefits, including more affordable devices, faster data rates, and enhanced multimedia features. .. Our approach is based on FDS. In this initial experiment, we are utilizing the proposed approach on the LMR and compatible cellular networks. The two dynamic schedulers, FDS and IDS, reduce packet loss and latency. The proposed method is novel in interoperable cellular and LMR networks, and it is the first to solve packet delay and loss in the heterogeneous mobile wireless network. The proposed scheduler works well to provide availability and quality of service (QoS) for disaster responders. Our approach was also used for high resource use in the same network. The enhanced characteristics of 5G mobile wireless network systems bring with them new security challenges and requirements .A comprehensive overview of 5G security is given in this article .Compared to traditional network topologies, wireless networks.

KEYWORDS: Packet loss, packet delay, and public safety land mobile radio interoperability, device-to-device 5G wireless security architecture

I. INTRODUCTION

Disaster responders need to coordinate and communicate with each other as soon as possible to save lives and property. In emergency situations, effective communication is crucial. Mobile wireless networks are now even more essential to disaster relief efforts due to recent advancements in wireless technologies. Land mobile radios (LMRs) are already used by public safety agencies for rapid emergency response and team coordination. In order to react and recover during a crisis, disaster responders must have effective communication. For example, having Internet access allows emergency responders to share multimedia information and engage in real-time communication with commanders and specialists located off- site. offer informed assistance. However, these communication features are not available with the current public safety LMRL service availability may be detrimental to lives in the public safety domain, but it also means lower revenue for commercial cellular networks. Therefore, it makes sense to enhance the interoperability of these two wireless networks to offer new multimedia services (including video), increased user data rates, and low-cost devices to disaster responders. The current 4G/international mobile telecommunications technology will be surpassed by the upcoming 5G mobile wireless telecommunications generation. Advanced Structures. In addition to offering many new service possibilities, the 5G wireless technology offers an improvement over the 4G older cellular networks. Mass machine-type and device-to-device (D2D) connections are some of the cutting-edge features that 5G research and development hopes to accomplish. These include increased density of mobile broadband users, better capacity than existing 4G, and more. The goal of 5G, the next generation of mobile wireless telecommunications, is to lower latency and energy consumption for improved Internet of Things (IoT)TH generation wireless systems, going beyond the existing 4G/International Mobile Telecommunications (IMT)-

A. Interoperable Cellular and Public Safety LMR

Given that natural catastrophes and terrorist attacks typically occur in limited areas, we assume that the cellular network covers the LMR. Disaster responders can access both the LMR and the cellular network within its service area by using multiple radio interfaces on their mobile devices. But commercial customers can only access the cellular network. Responders to disasters can obtain IP-based multimedia services, such as video streaming via the cellular network, and mission-critical services, such as tactical group voice, over the LMR. The handoff assistance between these two networks ensures continuous service continuity because disaster responders can easily wander across the interoperable LMR/cellular systems networks to increase service availability. Furthermore, the session should be migrated to cellular networks instead of terminating when a disaster responder departs the public safety LMR network's coverage region in order to preserve communication. For heterogeneous wireless networks, a few interoperability techniques have been created. For heterogeneous systems, the authors of offer a location management solution that incorporates location updates and paging. The optimal conditions for performing a vertical handoff are discussed. inside. To improve voice and data service performance in cellular/WLAN integrated networks, the authors of and look into various admission control systems. There are recommendations for scalable routing techniques in heterogeneous mobile networks.. When compared to commercial wireless cellular customers, the base of public safety LMR users is two orders of magnitude smaller. Because of this, the R&D costs associated with commercial wireless cellular networks are far higher than those associated with public.

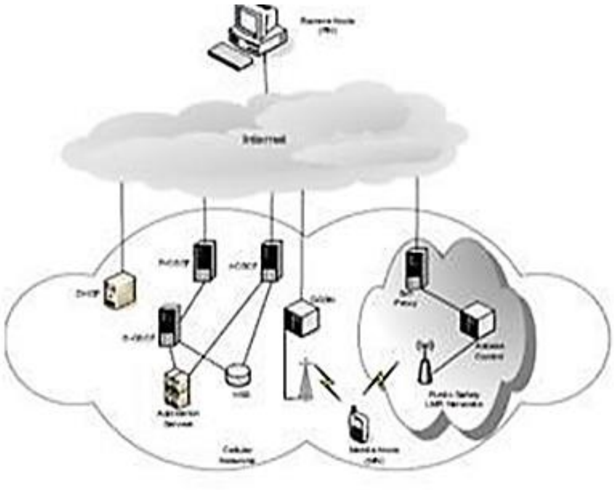

Figure 1: Interoperable Wireless Cellular and Public Safety LMR Networks

B. State of the Art

Several methods have been developed to enhance the interoperability between cellular and LMR networks, in contrast to the methods in previous studies. Session Initial Protocol (SIP) and a combined radio resource management architecture serve as the foundation for these techniques. SIP was developed by the Internet Engineering Task Force (IETF) to provide phone session management and multimedia application-layer signaling, thereby providing actual end-to-end mobility control. Moreover, SIP offers strong scalability and growth due to its use of text-based control messages and top- layer operation. MWIF, 3GPP, and 3GPP2 are among the wireless technical forums that have chosen to use SIP for session management. However, in traditional SIP-based handoff methods, the application layer message exchange might result in severe handoff delays.

II. RESEARCH APPROACH

This research project identifies the problem of disaster response and recovery in interoperable heterogeneous mobile wireless networks. This goal is accomplished by enhancing radio resource management and reducing packet loss and delay. We present our method for enhancing radio resource management: a dynamic scheduler with feedback that provides guarantees for service quality and availability and is based on discrete time control hypothesis .lowering handoff times and packet loss issues in various mobile wireless networks and preset

A. Feedback Dynamic Schedule

The FDS and IDS algorithms will be created using feedback control theory. Both techniques leverage HCCA features to distribute WLAN channel capacity to wireless stations hosting real-time applications, assuming that they are functioning at the HC. As a result, the HC can assign TXOPs to ACs in accordance with their distinct transmission queue levels and time constraints [13]. We will discuss a WLAN system made up of an access point and a number of quality-of-service enabled mobile stations (QSTAs). Each QSTA can have up to four queues. Let TCA be the interval of time between the start of two successive CAPs. At TCA intervals, the HC must allocate the bandwidth necessary to clear every queue during the ensuing CAP.,

$$q_i(n+1) = q_i(n) + d_i(n)T_{CA} + u_i(n)T_{CA}, \quad i = 1,\ldots,M \qquad (1)$$

where qi≥0, the queue level at the beginning of the nth CAP, and ui≤0, the average depletion rate (i.e., its absolute value denotes the bandwidth assigned to drain the queue) are all supplied. Di(n)=dis-dicp(n) represents the difference between the average input rate at the queue during the nth TCA interval, di(n)≥0, and the average output rate at the queue during the nth TCA interval, diCP(n)≥0. The input di(n) is unpredictable since it depends on how many packets are broadcast and how the source feeding the ith queue behaves.

Therefore, from the perspective of control theory, di(n) can be regarded as a disturbance [25]. Without losing generality, the piece-wise constant model for the disturbance di(n) that follows can be accepted for given.

$$d_i(n) = \sum_{j=0}^{+\infty} d_{0j} \cdot 1(n - t_j) \qquad (2)$$

Therefore, from the perspective of control theory, di(n) can be regarded as a disturbance [25]. Without losing With due generality, the piece-wise constant model that follows for the disturbance di(n) can be taken as given. will only consider a step disturbance in the process of creating the feedback control rule, di(n)=d0.1(n).

B. Closed-Loop Control Scheme

Our goal is to develop a control law that sets the target value Tit, which represents the desired quality of service (QoS) for that queue by the AC, higher than the queuing delay Ti that each frame in the nth queue experiences. We will examine the closed loop control system shown in Fig. 2, where the set point qiT has been set to zero, thus ideally we would aim for empty queues.

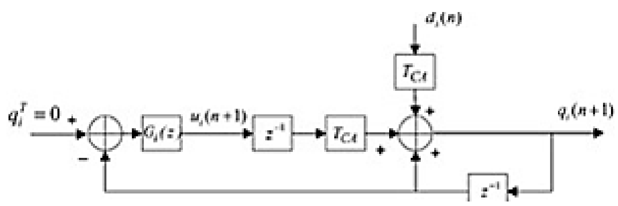

Figure 2: Closed Loop Control Scheme

Regarding the transfer function Gi(z) of the controller, we will focus on two very fundamental controllers: a proportional (P) controller Gi(z)=kpi and a proportional-integral (PI) controller. Gi(z)=kpi.(1+z/z-1, 1/TIi)

C. Computational Complexity of the Bandwidth Allocation Algorithms

Here is an estimate of the computational complexity of the recommended allocation methods. First Proposition: In a WLAN system with M active traffic streams, the computing complexity of the FDS approach is O(2M). Proof: At each time interval TCA, the HC assigns a certain amount of bandwidth to each of the M active traffic streams.

III. EVALUATION AND PRELIMINARY RESULTS

Table I displays the total TXOPs allotted during CAPs during the super frame period, which is the average and peak super frame usage in HCCA mode. It shows that, on average, the Simple scheduler consumes the most WLAN resources. The issue is that, although providing a CBR service, the quota of resources allotted is not adjusted by the basic scheduler to reflect the actual demand. It is feasible to monitor the bandwidth requirements of real-time flows and use bandwidth more wisely thanks to control systems. packet lag. Different security levels must be taken into account for various circumstances for each security service; if differentiated security is provided, a flexible security architecture is required.

Depending on the use cases, several network functions in the control plane are included in our suggested security architecture. Flexible security measures based on PCF requirements are offered by AMF and SMF. Rather than using a single strategy to support all applications, the security setup needs to be tailored and optimized for each unique application.

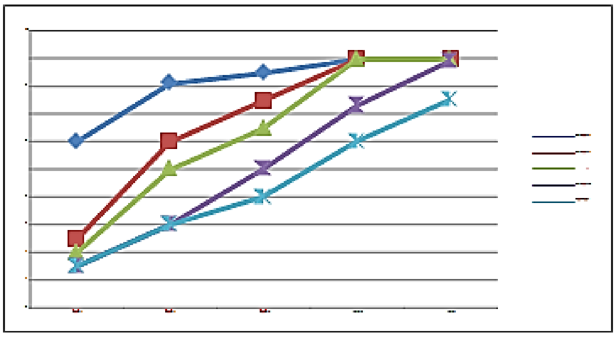

Figure 3: Result shows the proposed control strategies enable more appropriate bandwidth use

The peak superframe utilizations of the Simple scheduler at high traffic loads (α = 10 and α = 12) are lower than those provided by IDS and FDS for the same reason. This result clearly shows that the proposed control strategies enable more appropriate bandwidth use and enable real-time flow bandwidth requirements to be tracked.

Table 1: Result

α	IDS ($k_{p_i} = 15s^{-1}, T_{I_i} = 4$)			FDS			SS		
	Superframe Utilization		Overall Goodput	Superframe Utilization		Overall Goodput	Superframe Utilization		Overall Goodput
	Average [%]	Peak [%]	FTP flows [Mbps]	Average [%]	Peak [%]	FTP flows [Mbps]	Average [%]	Peak [%]	FTP flows [Mbps]
5	6.8	29.5	4.57	6.95	31	4.58	25.62	32.42	4.57
10	15.2	80.2	4.33	15.22	82	4.38	52.4	62.58	4.27
12	29.3	80.9	2.52	17.66	80	4.09	63.75	74.98	2.32

A. Generic Architecture For 5g Wireless Systems

The fifth generation mobile network, often known as a 5G network, is a new worldwide wireless standard that may provide peak data rates of up to 20 gigabits per second (Gbps) and average data rates of more than 100 megabits per second (Mbps). These networks follow 1G, 2G, 3G, and 4G networks. In 5G, bonded up to 800 MHz channels with orthogonal frequency-division multiplexing (OFDM) encoding will be employed .Since the mobile world has evolved beyond what it is, 5G addresses all communication services. Its scope extends beyond mobile communication. Actually, by making all kinds of services available voice and non-voice, critical and non-critical, and Internet of Things, it is genuinely advancing the digital world's future. Promoting the change of the economy in all areas and utilizing a variety of technologies (Wi-Fi,) 4G, and new radio technologies).

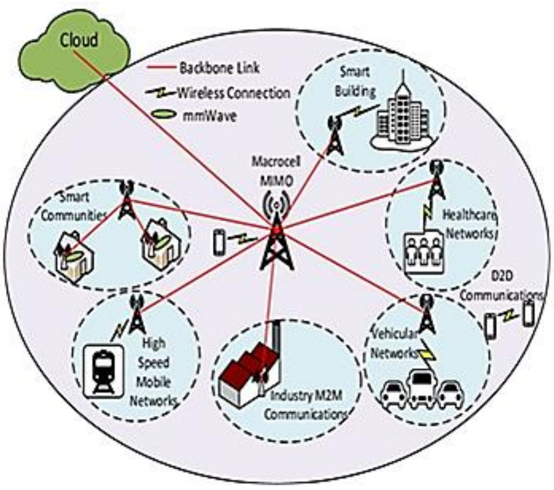

Figure 4: 5G network

Table 1: Security requirements for 5G wireless networks

Specifications with regard to 4G	Improve resilience and availability of the network against signaling based threats including overload caused maliciously or unexpectedly
	Specific security design for use cases which require extremely low latency
	Comply with security requirements defined in 4G 3GPP standards. Need to apply especially to a virtualized implementation of the network
	Provide Public Safety and Mission Critical Communications (resilience and high availability)
Requirements from the standpoint of radio access	Improve system robustness against smart jamming attacks
	Improve security for 5G small cell nodes

Among the many particular needs that can be relevant to the new use cases is ultra-low latency in user communications. New technologies enable advanced service capabilities, but they also open up a window for weaknesses, which places additional security restrictions on 5G. varied access technologies in HetNet may demand varied security requirements, and a multi network environment may need very frequent authentications with stringent delay constraints. One of the most important 5G technologies to achieve improved both as well as spectrum-efficient. It's also seen to be a practical strategy to avoid listening in silence. Additionally, SDN and NFV in 5G will make new services possible. distribution models, making the inclusion of fresh security elements necessary. The concepts of five-component of the overall architecture to deal with these issues. To enable a variety of use cases and new trust models in the best possible way, flexible security solutions are needed. The trust models for older cellular networks and 5G wireless networks are shown in In 5G wireless networks, authentication is required not just between service providers but also between subscribers and the two operators (the residential and auxiliary networks). Additionally, there may be significant differences in the security needs for different applications within the vertical industries use case. .. As an illustration, mobile Devices require lightweight security mechanisms due to power limits, whereas high-speed services require low-latency and efficient security services. Therefore, the wide flexibility of 5G security measures is another critical requirement. The complexity of authentication management increases with the variety and sheer quantity of 5G devices that are linked. Different applications can make use of different authentication models. User authentication may be handled by the network provider or the service provider.

The security research projects are described in this part from the perspective of 5G-related technology. First, we provide a brief synopsis of the 5G technology. The security functions of each Next Each technology are described. The technologies utilized in 5G wireless networks, such as massive MIMO, HetNet, D2D, SDN, and IoT, are covered in this section.

IV. CONCLUSION

We have looked into the problem of interoperability in commercial cellular networks for public safety LMR networks and disaster response. Interoperability can be enhanced by S- SIP and optimal radio resource management. We have suggested the Feedback dynamic scheduler technique to optimize overall radio resource consumption while ensuring QoS, e.g., lower packet loss. To investigate further quality of service specifications for LMR and compatible cellular wireless networks, more research is being conducted.

CONFLICT OF INTERREST

The authors declare that they have no conflict of interest.

REFERENCES

[1] "TIA/EIA Telecomm. Syst. Bull.,TSB102-A," TIA/ApcoProject 25 System and Standards Definition
[2] H. Holma and A. Toskala, WCDMA for UMTS: Radio Access for Third Generation Mobile Communications. Wiley, New York, 2004.
[3] J. Gozalvez, "HSDPA goes commercial," IEEE Vehicular Technology Magazine, vol. 1, pp. 43–53, March 2006.
[4] S. Frattasi, H. Fathi, F. Fitzek, R. Prasad, and M. D. Katz, Defining 4G technology from the user‘s perspective," January 2006 issue of IEEE Network.
[5] Balachandran, K. C. Budka, T. P. Chu, T. L. Doumi, and J.
H. Kang, Mobile responder communication networks for public safety," IEEE Commun. Mag., pp. 56-64, 2006.
[6] "Mobility management in heterogeneous wireless networks," Assouma, R. Beaubrun, and S. Pierre, IEEE J. Select. Areas Commun., vol. 24, pp. 638-648, Mar. 2006.
[7] "An MDP-based vertical handoff decision algorithm for heterogeneous wireless networks," Stevens-Navarro, Y. Lin, and V. W. S. Wong, vol. 57, pp. 1243-1254, Mar. 2008.
[8] Performance investigation of the WLAN-first strategy in cellular/WLAN internetworking, W. Song, H. Jiang, and W. Zhuang, vol. 6, pp. 1932-1952, May 2007.
[9] W. Song, Y. Cheng, and W. Zhuang, Improving voice and data services in cellular/WLAN integrated networks by admission control," vol. 6, pp. 4025-4037, Nov. 2007.
[10] "SMART: scalable mobility adaptive routing techniques for heterogeneous mobile networks," by T. Yagyu, M. Jibiki, and K. Yoshida, in Proc. IEEE WCNC'07, 2007.
[11] J. Rosenberg and et al., SIP: session initiation protocol," IETF RFC 3261, June 2002.
[12] W.Stallings,"Cryptography and Network Security Principles and Prac-tice Sixth Edition", PEARSON, 2014.
[13] "5G scenarios and security design", HUAWEI, 2016.
[14] "5G security recommendations package network slicing", NGMN
[15] S. Vij, and A. Jain, "5G: Evolution of a secure mobile technology",2016 3rd International Conference on Computing for Sustainable GloblDevelopment (INDIACom), 2015, pp. 2192-2196.
[16] Z. Qin, Y. Liu, Z. Ding, Y. Gao, and M. Elkashlan, "Physical Layer Se-curity for 5G Non-orthogonal Multiple Access in Large-scale Networks",2016 IEEE International Conference on Communications (ICC), 2016,Alliance, April, 2016.

ABOUT THE AUTHOR

Satya Prakash Adim Received his B.Tech Degree in Computer Science Engineering in 2013. He is M.Tech student in Department of Computer Science Engineering, Dr AKTU University Lucknow His current research interests in network security,network design, network modelling, simulation and performance analysis for next generation wireless networks, wireless ad-hoc and sensor networks