HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN HỒNG THỦY

NGHIÊN CỨU GIẢI PHÁP KỸ THUẬT ĐỊNH VỊ THIẾT BỊ DI ĐỘNG THẾ HỆ THỨ TƯ VÀ ỨNG DỤNG CHO CÔNG TÁC AN NINH

LUẬN ÁN TIẾN SĨ KỸ THUẬT VIỄN THÔNG

Hà Nội, tháng 10 năm 2023

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN HỒNG THỦY

NGHIÊN CỨU GIẢI PHÁP KỸ THUẬT ĐỊNH VỊ THIẾT BỊ DI ĐỘNG THẾ HỆ THỨ TƯ VÀ ỨNG DỤNG CHO CÔNG TÁC AN NINH

Chuyên ngành: **Kỹ thuật viễn thông**

Mã số: **9.52.02.08**

LUẬN ÁN TIẾN SĨ KỸ THUẬT VIỄN THÔNG

NGƯỜI HƯỚNG DẪN KHOA HỌC

PGS.TS. Lê Nhật Thăng

TS. Hồ Văn Canh

Hà Nội, tháng 10 năm 2023

LỜI CẢM ƠN

Với lòng kính trọng và biết ơn sâu sắc, tôi xin chân thành cảm ơn Phó Giáo sư, Tiến sĩ Lê Nhật Thăng và Tiến sĩ Hồ Văn Canh, các Thầy đã tận tình hướng dẫn, giúp đỡ tôi trong suốt quá trình nghiên cứu sinh và làm luận án.

Xin chân thành cảm ơn Ban Giám đốc Học viện Công nghệ Bưu chính Viễn thông, Khoa Đào tạo Sau Đại học Học viện; Lãnh đạo Bộ Công an, Bộ Thông tin và Truyền thông; Lãnh đạo Cục Kỹ thuật nghiệp vụ - Bộ Công an đã tạo điều kiện, giúp đỡ, hỗ trợ và động viên tôi trong suốt quá trình học tập, nghiên cứu, khảo sát và thử nghiệm thực tế phục vụ công trình nghiên cứu này.

Xin cảm ơn gia đình, bạn bè, đồng nghiệp và nhiều Nhà khoa học có uy tín khác đã động viên, hỗ trợ và đóng góp ý kiến để tôi có thể hoàn thành công trình nghiên cứu và luận án này.

Dù đã rất cố gắng nhưng với thời gian nghiên cứu, thời gian thực tế có hạn, trong khi đó khoa học và công nghệ, đặc biệt là công nghệ di động, công nghệ xử lý dữ liệu có nhiều sự thay đổi, phát triển vượt bậc nên chắc chắn công trình này còn không tránh khỏi những thiếu sót, bất cập. Tôi rất mong nhận được sự chỉ dẫn, góp ý tiếp của các Thầy, các Nhà khoa học, Lãnh đạo các cơ quan, đồng nghiệp và bạn đọc để luận án của tôi được tiếp tục phát triển, đóng góp một phần cho sự phát triển khoa học công nghệ đất nước và ứng dụng thực tế có hiệu quả cho ngành Công an.

Nghiên cứu sinh xin chân thành cảm ơn./.

Hà Nội, ngày tháng 10 năm 2023

Nghiên cứu sinh

Nguyễn Hồng Thuỷ

LỜI CAM ĐOAN

Tôi xin cam đoan Công trình nghiên cứu, luận án tiến sĩ ***"Nghiên cứu giải pháp kỹ thuật định vị thiết bị di động thế hệ thứ tư và ứng dụng cho công tác an ninh"*** là công trình nghiên cứu của riêng tôi.

Các kết quả nghiên cứu là trung thực và chưa từng công bố trong bất kỳ công trình nào khác.

Các cơ sở khoa học, toán học; nguyên lý kỹ thuật, công nghệ; phần mềm và thuật toán cơ sở; số liệu khảo sát thực tế đều được tôi trích dẫn, tham chiếu, ghi chú. Nếu có bất cứ cơ sở khoa học và số liệu thực tiễn nào còn chưa được trích dẫn, tham chiếu, ghi chú là do sơ xuất của tôi, kính mong các Tác giả, các Nhà khoa học và Bạn đọc tiếp tục chỉ dẫn, góp ý giúp để tôi bổ sung, chỉnh sửa.

Nghiên cứu sinh xin chân thành cảm ơn./.

Hà Nội, ngày tháng 10 năm 2023

Nghiên cứu sinh

Nguyễn Hồng Thuỷ

MỤC LỤC

BẢNG THUẬT NGỮ VIẾT TẮT

TT	Tên viết tắt	Tiếng Anh	Tiếng Việt
1.	1G/2G/3G/4G /5G	1st/2nd/3rd/4th/5th Generation	Mạng thông tin di động thế hệ thứ nhất/ thứ hai/ thứ ba/ thứ tư/ thứ năm
2.	3GPP	3rd Generation Partner Project	Dự án hợp tác phát triển di động
3.	911		Dịch vụ cứu hộ khẩn cấp của Mỹ và Canada (thông qua nhắn tin và định vị di động)
4.	AI/ML	Artificial Intelligence/ Machine Learning	Trí tuệ nhân tạo/Học máy
5.	A-GNSS/A-GPS	Assistant Global Navigation Satellite System/Assistant Global Positioning System	Hệ thống vệ tinh dẫn đường/Định vị toàn cầu được trợ giúp
6.	AFLT	Advanced Forward Link Trilateration	(Kỹ thuật định vị) đo đa phương (đo tam giác) liên kết chuyển tiếp nâng cao
7.	AoA	Angle of Arrival	Góc đến của tín hiệu
8.	Algorithm		Thuật toán
9.	ALI	Automatic Location Identification	Tự động nhận dạng vị trí
10.	AMPS	Analog Mobile Phone System	Hệ thống thông tin di động (kỹ thuật tương tự)
11.	Analog		Kỹ thuật tương tự
12.	AP	Access Point	Điểm truy cập Wifi
13.	API	Application Programming Interface	Giao diện lập trình ứng dụng
14.	AP-RSSI	Access Point Received Signal Strength Indication	Kỹ thuật định vị dựa trên chỉ báo cường độ tín hiệu nhận được (cho Wifi)

TT	Tên viết tắt	Tiếng Anh	Tiếng Việt
15.	ARFCN	Absolute Radio Frequency Channel	Kênh tần số vô tuyến tuyệt đối (cho mạng di động)
16.	Beidou	Beiou GNSS	Hệ thống vệ tinh dẫn đường toàn cầu của Trung Quốc
17.	Big Data		Dữ liệu lớn
18.	BS	Base Station	Trạm gốc (di động)
19.	BSC	Base Station Controller	Bộ điều khiển trạm gốc
20.	BSS	Base Station Subsystem	Phân hệ trạm gốc
21.	BTS	Base Transceiver Station	Trạm gốc (thu phát) thông tin di động
22.	C4I	Command, Control, Communications, Computers, Intelligence System	Hệ thống thông minh máy tính, truyền thông, điều khiển, chỉ huy
23.	Cell ID/CID	Cellular Identity	Số định danh ô di động
24.	CI+TA	Cell ID + Timming Advanced	Kỹ thuật định vị Cell ID kết hợp định thời tiên tiến
25.	CAND		Công an nhân dân (Việt Nam)
26.	CDR	Call Detail Record	Bản ghi chi tiết cuộc gọi
27.	Cell	Cellular	Tế bào (di động)
28.	CERP	Cicle Error Probability	Xác xuất sai số hình tròn
29.	CQAN		Cơ quan an ninh (Việt Nam)
30.	CDMA/ FDMA/ TDMA	Code Division Multi Access/Frequency Division Multi Access/ Time Division Multi Access	Đa truy cập phân chia theo mã/theo tần số/theo thời gian
31.	Data Lake		Hồ dữ liệu

TT	Tên viết tắt	Tiếng Anh	Tiếng Việt
32.	Digital		Kỹ thuật số
33.	DL	Down Link	Đường xuống
34.	DW	Data Warehouse	Kho dữ liệu
35.	E911	Enhanced 911	Dịch vụ cứu hộ khẩn cấp của Mỹ và Canada được nâng cao
36.	eNodeB (eNB)		Trạm gốc 4G-LTE
37.	EOTD	Enhanced Observed Time Difference	Chênh lệch thời gian quan sát được nâng cao (kỹ thuật định vị)
38.	E-TDoA	Enhanced-TDoA	Đo chênh lệch thời gian đến tiên tiến
39.	ETSI	Euro Telecommunication Standard Institude	Viện tiêu chuẩn viễn thông Châu Âu
40.	E-UTRAN	Evolved Universal Terrestial Radio Access Network	Mạng truy nhập vô tuyến mặt đất đa năng được nâng cấp
41.	FCC/FDD	Federal Communication Commission/ Frequency Division Duplexing	Uỷ ban truyền thông liên bang (Mỹ)/Song công phân chia theo tần số (LTE hỗ trợ)
42.	Glonass	Glonass GNSS	Hệ thống vệ tinh dẫn đường toàn cầu của Nga
43.	Galileo	Galileo GNSS	Hệ thống vệ tinh dẫn đường toàn cầu của Châu Âu
44.	Gbps	Gigabit per second	(Tốc độ dữ liệu) giga bít/giây
45.	GSM	Global System for Mobile	Hệ thống thông tin di động (kỹ thuật số) toàn cầu
46.	HLR/VLR	Home Location Register/ Visitor Location Register	Bộ đăng ký vị trí nhà (thuê bao nhà)/Bộ đăng ký vị trí khách (thuê bao khách)

TT	Tên viết tắt	Tiếng Anh	Tiếng Việt
47.	ID	Identification/ Identify/ Identity	Nhận dạng
48.	IMSI/IMEI/ TMSI	International Mobile Subscriber Identity/ International Mobile Equipment Identity/ Temporary Mobile Subscriber Identity	Số nhận dạng thuê bao di động quốc tế/Số nhận dạng thiết bị di động quốc tế/Số nhận dạng thuê bao di động tạm thời
49.	IoT/ IP	Internet of Things/ Internet Protocol	Internet vạn vật/ Giao thức Internet
50.	ITU	International Telecommunication Union	Liên minh Viễn thông Quốc tế
51.	LAC	Local Area Code	Mã vùng di động
52.	LBS	Location Base Services	Dịch vụ dựa trên vị trí
53.	LF	Location Fingerprints	Kỹ thuật định vị lấy dấu vân tay vị trí
54.	LI	Lawfull Interception	Thu chặn hợp pháp
55.	LNA	Low Noise Amplifier	Bộ khuếch đại tạp âm thấp
56.	LSB	Least Significant Bit	Bít có ý nghĩa thấp nhất
57.	LTE	Long Term Evolution	Công nghệ di động 4G cách mạng thời kỳ dài
58.	MAC	Media Access Control Address	Địa chỉ mạng máy tính
59.	MAP		Bản đồ
60.	Mbps	Megabit per second	(Tốc độ dữ liệu) mega bít/giây
61.	MCC	Mobile Country Code	Mã nước di động
62.	MLAT	Multilateration	Kỹ thuật đo đa phương (hay kỹ thuật định vị hyperpolic)
63.	MNC	Mobile Network Code	Mã mạng di động

TT	Tên viết tắt	Tiếng Anh	Tiếng Việt
64.	MD/ MP/ MS	Mobile Device/Phone/ Station	Thiết bị di động/ Điện thoại di động/ Máy (trạm) di động
65.	MSC	Mobile Switching Center	Trung tâm (tổng đài) chuyển mạch di động
66.	NCS		Nghiên cứu sinh
67.	NSA	National Security Agency	Cơ quan an ninh quốc gia (Mỹ)
68.	NSS	Network Switching System	Hệ thống chuyển mạch mạng
69.	ODS	Operation Data Store	Lưu trữ cơ sở dữ liệu hoạt động
70.	OFDM	Orthogonal frequency-division multiplexing	Điều chế phân chia theo tần số trực giao
71.	ODF	Open Data Flatform	Nền tảng dữ liệu mở
72.	OpenData		Dữ liệu mở
73.	OpenSourse		Nguồn mở
74.	OTT	Over The Top	Dịch vụ viễn thông dựa trên mạng
75.	OTDoA	Observed Time Difference of Arrival	Chênh lệch thời gian đến quan sát được (thuật toán)
76.	OTDoA-IPDL	Observed Time Difference of Arrival – Idle Period in Down Link	Kỹ thuật định vị dựa trên chênh lệch thời gian đường xuống
77.	PA	Power Amplifier	Bộ khuếch đại công suất
78.	PCI	Physical Cell ID	Định danh tế bào vật lý
79.	PMLN	Public Mobile Land Network	Mạng di động mặt đất công cộng
80.	QoS	Quanlity of Service	Chất lượng dịch vụ
81.	RAN	Radio Access Network	Mạng truy nhập vô tuyến

TT	Tên viết tắt	Tiếng Anh	Tiếng Việt
82.	RAW		Dữ liệu thô
83.	RF/RNC	Radio Frequency/ Radio Network Controller	Tần số vô tuyến điện/Bộ điều khiển mạng vô tuyến di động
84.	RSSI	Received Signal Strength Indication	Chỉ báo cường độ tín hiệu nhận (trong Wifi)
85.	RTD	Return Time Difference	Chênh lệch thời gian khứ hồi
86.	RTT	Round Trip Time	Độ trễ khứ hồi
87.	RMSE	Root Mean Square Error	Hàm điểm: căn bậc hai của sai số bình phương trung bình
88.	Rx-Level	Receiving Level	Mức thu
89.	SDR	Software Defined Radio	(Thiết bị) Vô tuyến định nghĩa bằng phần mềm
90.	SERP	Sphere Error Probability	Xác xuất sai số hình tròn
91.	SIB	System Information Block	Khối thông tin hệ thống
92.	SIM/srsRAN	Subscriber Identity Module/ Software Radio System for eNodeB/ for Radio Access Network	Thẻ nhận dạng di động/ Phần mềm (mã nguồn mở) lập trình cho thiết bị vô tuyến định nghĩa bằng phần mềm SDR từ hãng SRS hỗ trợ cho mạng truy nhập vô tuyến eNodeB 4G/5G.
93.	SS7	Signalling System No.7	Hệ thống báo hiệu số 7
94.	TA	Timming Advance	Định thời tiên tiến
95.	TAC	Tracking Area Code	Mã khu vực theo dõi
96.	TDD	Time Division Duplexing	Song công phân chia theo thời gian (LTE hỗ trợ)
97.	TDoA	Time Difference of Arrival	Chênh lệch thời gian đến (của tín hiệu)

TT	Tên viết tắt	Tiếng Anh	Tiếng Việt
98.	ToF	Time of Fly	Thời gian bay (của tín hiệu)
99.	ToT	Time of Transmission	Thời điểm phát (của tín hiệu)
100.	Tx-level	Transmitting Level	Mức phát
101.	UE	User Equipment	Thiết bị người dùng
102.	UL	Up Link	Đường lên
103.	UMTS	Universal Mobile Telecommunication System	Hệ thống viễn thông di động đa năng
104.	U-TDoA	Uplink Time Difference of Arrival	Chênh lệch thời gian đến của đường lên
105.	Wifi	Wireless Fidelity	Kết nối Internet băng rộng không dây ở khoảng cách ngắn
106.	Wimax	Worldwide Interoperability for Microwave Access	Tiêu chuẩn IEEE cho việc kết nối Internet băng thông rộng không dây ở khoảng cách lớn (qua sóng vi ba)
107.	WPS	Wifi Positioning System	Hệ thống định vị Wifi

BẢNG CÁC KÝ HIỆU TOÁN HỌC

TT	Ký hiệu	Ý nghĩa
1	k, n	Số nguyên dương
2	$\sqrt{}$	Căn bậc hai
3	$\frac{1}{n}$	Thương của phép chia 1 cho n
4	$\sum$	Tổng tất cả các giá trị của dãy số
5	$x_{mesuredk}$	Giá trị của phép đo vị trí thứ k
6	x_{true}	Vị trí thực tế của thiết bị di động được đặt
7	RMSE (.)	Hàm điểm: căn bậc hai của sai số bình phương trung bình (Root Mean Square Error)
8	$A_1, A_2, \ldots A_k$	Các tập hợp
9	$\varnothing$	Tập hợp rỗng (tập hợp không chứa phần tử nào)
10	$\cap$	Phép giao của các tập hợp
11	$\cup$	Phép hợp của các tập hợp
12	M	Số lượng ăng-ten của mảng gồm các ăng-ten cách đều nhau
13	d	Khoảng cách giữa 2 ăng-ten liên tiếp của mảng ăng-ten gồm M ăng-ten cách đều nhau
14	L	Khoảng cách đường truyền của tín hiệu nhận được ở ăng-ten
15	θ	Góc đến của tín hiệu đa đường so với pháp tuyến của dải ăng-ten của điểm truy cập Wifi
16	θ_k	Góc đến của tín hiệu đường truyền thứ k so với pháp tuyến của dải ăng-ten của điểm truy cậpWifi
17	sin (.)	Hàm sin (hàm lượng giác cơ bản)
18	π	Hằng số Archimedes - *pi* (có giá trị xấp xỉ bằng 3,14)

TT	Ký hiệu	Ý nghĩa
19	Exp (.)	Hàm lũy thừa của e với số mũ nào đó (trong đó e là cơ số của logarit tự nhiên có giá trị xấp xỉ bằng 2,71828)
20	$(.)^{T}$	Phép chuyển vị của ma trận
21	$\vec{\mathbf{x}}$	Véc tơ tín hiệu nhận được
22	$\vec{\Gamma}$	Độ suy giảm phức của vectơ dọc theo đường truyền *L*

DANH MỤC CÁC HÌNH VẼ

DANH MỤC CÁC BẢNG BIỂU

MỞ ĐẦU

Khái quát về công trình nghiên cứu

Trong luận án này, khái niệm thiết bị di động (MD) sẽ được đồng nhất với điện thoại di động (MP), hay trạm di động (MS) hay thiết bị người dùng (UE) tùy theo ngữ cảnh trình bày. Một số khái niệm như kỹ thuật định vị, công nghệ định vị hay phương pháp/ giải pháp định vị đôi khi cũng được dùng cùng một nghĩa, tùy theo ngữ cảnh.

Định vị thiết bị di động (hay định vị điện thoại di động, định vị di động) có tầm quan trọng và ý nghĩa to lớn, thiết thực trong công nghệ viễn thông di động; trong các lĩnh vực kinh tế, xã hội, an ninh công cộng và đời sống con người. Ngay khi thiết lập mạng viễn thông di động, kỹ thuật định vị đã được nghiên cứu áp dụng để mạng di động xác định được vị trí của thuê bao và phục vụ. Trong quá trình hoạt động, mạng di động phải thực hiện nhiều phương pháp định vị để phục vụ các yêu cầu dịch vụ, điển hình như cung cấp các dịch vụ dựa trên vị trí (LBS). Ta có thể thấy, một trong những ứng dụng rộng rãi, có giá trị nhất của định vị thiết bị di động trong kinh tế, xã hội, chuyên dùng và đời sống là dẫn đường. Trong an ninh công cộng, định vị thiết bị di động đặc biệt cần thiết cho thông tin chỉ huy, điều hành; thông tin khẩn cấp và cứu hộ cứu nạn; giám sát an ninh công cộng và nhiều hoạt động khác. Do vậy, kỹ thuật, công nghệ và các ứng dụng của định vị thiết bị di động là lĩnh vực luôn được quan tâm nghiên cứu, phát triển.

Những năm gần đây, công nghệ điện tử và viễn thông di động đã có sự phát triển nhanh chóng, vượt bậc. Thế giới đã trải qua 4 thế hệ công nghệ di động 1G/2G/3G/4G và hiện đang phát triển 5G, một số nước đã bắt đầu nghiên cứu về 6G. Ở nước ta, kể từ khi có mạng di động đầu tiên với công nghệ tương tự APMS (hệ thống Callink tại TP. Hồ Chí Minh) vào đầu những năm 1990, sau đó là mạng di động số GSM của Mobifone từ năm 1994, đến nay đã có 5 nhà mạng di động cung cấp dịch vụ: Mobifone, VNPT-Vinaphone, Viettel Mobile, Vietnammobile và Gtel Mobile. Trong đó, Gtel Mobile chỉ cung cấp rất hạn chế 2G; Vietnammobile cũng cung cấp hạn chế 2G, 3G; ba nhà mạng còn lại chiếm thị phần chính và cung cấp đầy đủ 2G, 3G, 4G với vùng phủ sóng rộng rãi trên toàn quốc. Ba nhà mạng này cũng đang thử

nghiệm triển khai 5G ở một số tỉnh, thành phố. Hiện chúng ta đang chuẩn bị đấu giá băng tần 5G và phát triển cung cấp dịch vụ 5G trong thời gian tới.

Có thể gọi mạng di động hiện nay là một mạng hỗn hợp cung cấp dịch vụ cùng lúc cả 3 thế hệ 2G/3G/4G. Cùng với sự ra đời của các công nghệ mới, tiên tiến như điện thoại thông minh, máy tính bảng, mạng Wifi công cộng, các dịch vụ gọi thoại và nhắn tin miễn phí, bảo mật trên nền mạng di động - Internet. Có thể nói, kết nối di động băng rộng 3G/4G/Wifi hiện nay đã phổ biến đến đa số người dân, doanh nghiệp, chuyên dùng. Một thiết bị di động bất kỳ như điện thoại thông minh, máy tính bảng, máy tính xách tay hay bất cứ modul chuyên dùng nào có gắn Sim 4G đều có thể cùng lúc hoạt động được với đa mạng băng rộng 3G/4G/LTE/Wifi và 2G ở bất cứ đâu trong vùng phủ sóng. Một cá nhân, đôi khi sở hữu nhiều thiết bị di động để liên lạc, kết nối, truy nhập cho nhiều mục đích khác nhau. Hiện đã có nhiều dòng điện thoại di động mới hỗ trợ 5G. Trong đó, có rất nhiều thuê bao/thiết bị kết nối có thể ẩn danh, ví dụ điển hình là khi sử dụng SIM rác, SIM Box, số ảo, các dịch vụ liên lạc trên nền mạng như Zalo, Viber, Whatsapp, Telegram, Messeger, Wechat v.v... Các trình bày ở sau đây sẽ sử dụng thuật ngữ định vị thiết bị di động thế hệ thứ tư hay định vị thiết bị di động 4G.

Những số liệu và thông tin sau được cung cấp trong [1] và [2]:

- Tính đến cuối Tháng 12/2022, tổng số thuê bao điện thoại của Việt Nam ước đạt **129,7** triệu thuê bao, tăng 3,1% so với cùng thời điểm năm trước, trong đó số thuê bao di động là **127,2 triệu**, tăng 3,7%; thuê bao truy nhập Internet băng rộng cố định ước đạt 21 triệu, tăng 8,6%.

- Trong Chiến lược quốc gia phát triển kinh tế số và xã hội số, mục tiêu phấn đấu đến năm 2025, tỉ lệ dân số đến độ tuổi trưởng thành có điện thoại thông minh đạt 95%.

Nếu đạt được mục tiêu đó, cùng với các mục tiêu về hạ tầng số và chuyển đổi số khác thì số lượng thuê bao di động thông minh sẽ đến hàng trăm triệu (vì mỗi người có thể sở hữu một hoặc nhiều thuê bao), tức là số thuê bao sử dụng dịch vụ di động băng rộng 3G/4G/Wifi và tiến tới là 5G sẽ rất lớn.

Sự phát triển nêu trên vừa là điều kiện thuận lợi cho phát triển kinh tế, xã hội của đất nước vừa là thách thức đối với công tác an ninh công cộng. Các đối tượng đang và sẽ triệt để lợi dụng sự phát triển của công nghệ, dịch vụ trên nền tảng điện thoại di động và không gian mạng vào hoạt động. **Việc tìm kiếm, xác định và truy vết** các đối tượng có hành vi xâm phạm an ninh, trật tự là hết sức cần thiết nhưng rất khó khăn khi chúng lợi dụng dịch vụ di động 4G để hoạt động. Bên cạnh đó, đối với các yêu cầu như tìm kiếm cứu hộ, cứu nạn, việc định vị thiết bị di động để tìm kiếm một người gặp nạn gặp nhiều khó khăn do độ khả dụng, thời gian định vị và độ chính xác định vị chưa đáp ứng yêu cầu. Các dịch vụ xã hội liên quan đến vị trí di động như dẫn đường, tiếp thị từ xa cũng gặp nhiều khó khăn, hạn chế. **Do vậy, định vị thiết bị di động 4G là một yêu cầu thực tế và cấp thiết.**

Qua nghiên cứu và khảo sát thực tế, đã có một số giải pháp kỹ thuật định vị di động nhưng hiện không có giải pháp kỹ thuật nào hiệu quả đối với yêu cầu định vị thiết bị di động 4G cho công tác an ninh. Một số nghiên cứu liên quan cũng đã chỉ ra điều này [3], [4], [27], [29], [38].

Đa phần, các nghiên cứu chuyên sâu, các tiêu chuẩn là riêng cho kỹ thuật mạng (để kết nối phục vụ thuê bao), ứng dụng của chính nhà mạng cung cấp (như LBS) [43, 44, 45], hay nhiều hơn nữa là các ứng dụng dịch vụ như Google Maps, cứu hộ cứu nạn như E911 của Mỹ và Canada [25]…Hiện chưa có công trình nghiên cứu khoa học nào đã được công bố giải quyết riêng, tổng hợp về vấn đề định vị thiết bị di động 4G ứng dụng cho công tác an ninh. Ngoài ra, luận án chưa tìm thấy một tài liệu khả dụng nào của các nhà cung cấp thiết bị chuyên dụng trên thế giới về lĩnh vực này. Một số nhà cung cấp có giới thiệu về giải pháp định vị di động 4G nói chung [35, 36, 55-58], nhưng chưa thấy bất cứ tài liệu khoa học, kỹ thuật cụ thể nào hoặc chỉ đưa ra được một phương án kỹ thuật với tác dụng còn rất hạn chế.

Do vậy, vấn đề cấp thiết hiện nay là nghiên cứu, tìm hiểu được một giải pháp kỹ thuật hiệu quả *(có tính khả thi, khả dụng, thời gian nhanh chóng và độ chính xác cao)* để định vị thiết bị di động 4G và nghiên cứu mô hình hệ thống kỹ thuật ứng dụng cho công tác an ninh. (Bên cạnh ứng dụng cho an ninh công cộng, định vị thiết bị di

động 4G cũng có thể ứng dụng rộng rãi cho các lĩnh vực khác như thông tin điều hành, chỉ huy, cứu hộ cứu nạn, dẫn đường v.v…).

Với tầm quan trọng, ý nghĩa của định vị thiết bị di động nêu trên, sự phát triển của công nghệ di động, căn cứ vào yêu cầu thực tế, NCS đã đề xuất và được giao thực hiện Đề tài luận án Tiến sĩ Kỹ thuật viễn thông: ***"Nghiên cứu giải pháp kỹ thuật định vị thiết bị di động thế hệ thứ tư và ứng dụng cho công tác an ninh"***.

Những vấn đề đặt ra cần nghiên cứu

Như đã phân tích ở trên, việc nghiên cứu đề tài luận án giải quyết cac yêu cầu sau đây:

- Định vị được thiết bị di động 4G một cách khả thi, khả dụng, nhanh chóng và chính xác. Giải pháp kỹ thuật và mô hình hệ thống định vị thiết bị di động 4G và ứng dụng của nó cho công tác an ninh trong thực tế.

- Các cơ sở khoa học, tính mới của giải pháp kỹ thuật, khả năng ứng dụng và hướng phát triển tiếp theo của giải pháp.

- Những đóng góp mới về mặt học thuật của luận án, ý nghĩa khoa học, thực tiễn của luận án.

Mục tiêu và phạm vi nghiên cứu của đề tài

* Mục tiêu của đề tài luận án là nghiên cứu, đề xuất giải pháp kỹ thuật có hiệu quả, từ đó xây dựng được mô hình hệ thống kỹ thuật tổng thể định vị thiết bị di động thế hệ thứ tư và ứng dụng cho công tác an ninh.

Trên cơ sở đó làm rõ các đóng góp khoa học và thực tiễn của kết quả nghiên cứu; tính mới, tính hiệu quả của giải pháp được đề xuất; đáp ứng yêu cầu của cơ quan an ninh, phù hợp với điều kiện thực tế và có khả năng mở rộng đáp ứng yêu cầu phát triển trong tương lai.

* Nhiệm vụ nghiên cứu cụ thể gồm **6 vấn đề** sau đây:

(1) Làm rõ những luận giải, lý giải trước đây của việc định vị di động, định vị thiết bị di động thế hệ thứ tư và yêu cầu ứng dụng cho công tác an ninh.

(2) Tìm hiểu tình hình nghiên cứu liên quan và các vấn đề đặt ra ở trong nước, ngoài nước; những mặt đã đạt được, còn tồn tại và hướng giải quyết.

(3) Cơ sở khoa học, các nguyên lý kỹ thuật định vị di động, các công nghệ định vị di động, các kỹ thuật và công nghệ có liên quan đến vấn đề đặt ra cần nghiên cứu.

(4) Phân tích, lựa chọn và đề xuất giải pháp kỹ thuật nhằm nâng cao hiệu quả định vị thiết bị di động, cụ thể là nâng cao tính khả thi, độ khả dụng, đảm bảo thời gian nhanh và tăng độ chính xác định vị.

(5) Đề xuất mô hình tổng thể hệ thống kỹ thuật định vị thiết bị di động thế hệ thứ tư cho công tác an ninh; thiết kế cấu trúc, chức năng, nguyên lý hoạt động của các hệ thống kỹ thuật liên quan, phù hợp với điều kiện thực tế.

(6) Thực nghiệm một số kỹ thuật để minh chứng cho tính khả thi của kết quả nghiên cứu.

Để đạt được những mục tiêu, nhiệm vụ nêu trên, đề tài luận án xác định các đối tượng nghiên cứu và giới hạn phạm vi nghiên cứu vào **4 vấn đề trọng tâm** sau:

(1) Cơ sở khoa học, lý thuyết, các nguyên lý kỹ thuật, công nghệ định vị di động và một số kỹ thuật, công nghệ liên quan, gồm: thu thập, xây dựng cơ sở dữ liệu định vị đa nguồn; cải thiện độ chính xác định vị; phân lớp, xác định đối tượng; bảo mật chuyển giao kết quả định vị và trạm gốc giả lập thu thập tham số IMSI/IMEI.

(2) Giải pháp kỹ thuật định vị nhằm nâng cao hiệu quả định vị thiết bị di động.

(3) Mô hình kiến trúc tổng thể hệ thống kỹ thuật định vị thiết bị di động ứng dụng cho công tác an ninh.

(4) Thực nghiệm một số kỹ thuật, bao gồm: thu thập, xây dựng cơ sở dữ liệu Cell-ID từ nguồn mở; cải tiến, mở rộng thuật toán định vị ToA, AoA; giả lập trạm gốc thu thập tham số IMSI/IMEI hỗ trợ tìm kiếm, định vị đối tượng.

Phương pháp nghiên cứu

- Kết hợp nghiên cứu lý thuyết, khảo sát và thực nghiệm trên cơ sở các tài liệu và dữ liệu thu thập được.

- Nghiên cứu cơ sở khoa học, nguyên lý, giải pháp kỹ thuật và mô hình hệ thống ứng dụng: phương pháp định tính. Trong đó, sử dụng hai mẫu:

+ Mẫu cho xây dựng giải pháp kỹ thuật xử lý định vị là cơ sở dữ liệu Cell-ID từ nguồn mở và tập dữ liệu tham số phục vụ ToA, AoA giả định.

+ Mẫu cho mô hình hệ thống ứng dụng dựa trên đặc điểm của các mạng di động cung cấp dịch vụ di động 2G, 3G, 4G.

- Đối với thực nghiệm: phương pháp kết hợp định tính và định lượng. Trong đó, có mẫu thực nghiệm thu thập dữ liệu Cell-ID từ nguồn mở, cải tiến, mở rộng một số thuật toán định vị lấy từ nghiên cứu và mẫu cho thiết bị giả lập trạm gốc thu thập tham số IMSI/IMEI lấy từ dữ liệu khảo sát, đo giao diện vô tuyến của mạng tại địa điểm thực nghiệm.

Ý nghĩa khoa học và thực tiễn của Luận án

Mục tiêu, nội dung và kết quả nghiên cứu đề tài luận án có ý nghĩa khoa học và thực tiễn như sau:

- Góp phần ứng dụng tiến bộ của khoa học kỹ thuật vào công tác đảm bảo an ninh, trật tự. Đồng thời, nội dung luận án cũng có thể làm tài liệu tham khảo, bổ sung giáo trình đào tạo, bồi dưỡng.

- Đề tài luận án vừa mang tính chất khoa học, kỹ thuật chuyên ngành định vị di động, vừa mang tính mới là đề xuất giải pháp kỹ thuật, mô hình hệ thống định vị thiết bị di động nhằm "nâng cao hiệu quả định vị thiết bị di động thế hệ thứ tư" và "ứng dụng cho công tác an ninh", trong điều kiện thực tế hiện nay và có thể mở rộng, phát triển trong tương lai. Đó là các đóng góp chính mà đề tài luận án đặt ra.

Tuy nhiên, do đề tài luận án có nội dung khá rộng, nên trong phạm vi này, luận án chỉ đi sâu vào nghiên cứu, giải quyết **4 vấn đề trọng tâm** như đã nêu trong mục đích, đối tượng và phạm vi nghiên cứu ở trên.

Bố cục Luận án

Luận án được tổ chức thành 04 Chương (theo 4 nội dung trọng tâm nghiên cứu đã đặt ra), ngoài phần mở đầu và kết luận.

* Mở đầu.

* Chương 1. Tổng quan về định vị di động.

Nội dung Chương 1 trình bày các vấn đề chủ yếu sau đây:

- Những định nghĩa, khái niệm chủ yếu liên quan đến đề tài luận án; ý nghĩa và tầm quan trọng của vấn đề cần nghiên cứu;

- Phân tích, đánh giá các nghiên cứu trước đây về định vị di động nói chung và định vị thiết bị di động 4G ứng dụng cho công tác an ninh nói riêng; xác định những tồn tại, hạn chế, khó khăn thách thức của vấn đề này và hướng giải quyết.

- Nghiên cứu tổng quan về các nguyên lý kỹ thuật định vị di động;

- Xác định yêu cầu về một số kỹ thuật liên quan (cải thiện độ chính xác định vị, phân lớp định vị, bảo mật, trạm gốc giả lập).

* Chương 2. Giải pháp kỹ thuật nâng cao hiệu quả định vị thiết bị di động.

Trên cơ sở các vấn đề tổng quan đã được nghiên cứu ở Chương 1, Chương 2 phân tích, đề xuất giải pháp kỹ thuật định vị trên cơ sở kết hợp đa dạng nguồn dữ liệu, cải thiện độ chính xác một số kỹ thuật định vị nhằm nâng cao hiệu quả định vị thiết bị di động, đáp ứng các yêu cầu đặt ra.

* Chương 3. Mô hình hệ thống kỹ thuật định vị thiết bị di động và ứng dụng cho công tác an ninh.

Nội dung Chương 3 trình bày sử dụng kết quả nghiên cứu giải pháp kỹ thuật ở Chương 2 để xây dựng mô hình tổng thể hệ thống kỹ thuật định vị thiết bị di động trên cơ sở sử dụng phân lớp định vị, bảo mật và trạm gốc giả lập ứng dụng cho công tác an ninh.

- Chương 4. Thực nghiệm.

Nội dung Chương 4 trình bày các kịch bản, kết quả và đánh giá một số thực nghiệm để minh chứng giải pháp kỹ thuật, mô hình hệ thống đã nghiên cứu, đề xuất.

- Kết luận

- Hướng nghiên cứu, phát triển luận án.

- Danh mục các công trình nghiên cứu liên quan đến đề tài luận án đã công bố.

- Danh mục tài liệu tham khảo.

- Phụ lục: Nội dung các công trình nghiên cứu liên quan đến đề tài luận án đã công bố.

CHƯƠNG 1. TỔNG QUAN VỀ ĐỊNH VỊ DI ĐỘNG

1.1. Khái quát về định vị di động và các ứng dụng của định vị

Theo vết (định vị) di động là việc xác định vị trí hoặc địa điểm của một máy điện thoại di động (hoặc một thiết bị di động) khi nó cố định hoặc di chuyển. Việc định vị điện thoại di động có thể được tính toán thông qua kỹ thuật đo đa sóng (tức đo khoảng cách khác nhau giữa một vài cột sóng di động của mạng với máy điện thoại di động trên cơ sở các tín hiệu sóng vô tuyến của nó) hoặc đơn giản hơn là qua vị trí GPS. Để xác định vị trí của điện thoại di động bằng kỹ thuật đo đa sóng, điện thoại phải phát ít nhất một tín hiệu chuyển vùng để liên hệ với cột sóng lân cận gần nhất nhưng không yêu cầu kích hoạt cuộc gọi.

Nguyên lý kỹ thuật để xác định vị trí một điện thoại di động thường dựa trên các nền tảng sau đây [23, 24, 26, 32, 33]:

- Trên cơ sở mạng;
- Trên cơ sở máy cầm tay;
- Trên nền tảng của SIM di động;
- Theo vị trí của điểm cung cấp Wifi;
- Trên cơ sở kỹ thuật định vị lai ghép.

Đối với mỗi thế hệ mạng di động và tính chất của thiết bị di động, về nguyên lý, sẽ sử dụng kỹ thuật định vị tương ứng hoặc lai ghép các kỹ thuật trên với nhau.

Hiện nay, khi mạng di động 4G phổ biến, một thiết bị đầu cuối 4G có thể hoạt động được ở nhiều chế độ khác nhau, và bài toán định vị thiết bị di động đó cũng sẽ khác nhau đối với từng thiết lập hoạt động. Đồng thời, mỗi ứng dụng của việc định vị thiết bị di động 4G cho nhà mạng, nhà cung cấp dịch vụ giá trị gia tăng, doanh nghiệp, các cơ quan quản lý Nhà nước, cứu hộ cứu nạn, an ninh công cộng cũng sẽ khác nhau.

Những ứng dụng điển hình của định vị di động có thể kể đến:

- Đối với nhà cung cấp dịch vụ di động, Internet và mạng xã hội, một trong những kỹ thuật và yêu cầu cơ bản là cần biết đối tượng sử dụng dịch vụ/thuê bao hay thiết bị di động đang ở đâu để kết nối và cung cấp dịch vụ. Một ví dụ khác điển hình,

hữu dụng nhất hiện nay chính là dịch vụ dựa trên vị trí LBS như dẫn đường, tìm đường của Google Map, Viet Map.

- Đối với các doanh nghiệp kinh doanh, đặc biệt trong kỷ nguyên kỹ thuật số, thời đại Cách mạng Công nghiệp 4.0, quá trình chuyển đổi số hiện nay, nếu biết khách hàng, đối tượng phục vụ của mình đang ở đâu thì đã nắm chắc được một phần cơ hội kinh doanh. Đối với các doanh nghiệp đặc thù như giao thông vận tải, logistics, thương mại điện tử, bưu chính công nghệ mới…nếu biết khách hàng, phương tiện, hàng hoá của mình đang ở đâu là sẽ giải quyết được bài toán quản lý, điều phối một cách hiệu quả.

- Đối với các cơ quan quản lý Nhà nước, tìm kiếm cứu hộ cứu nạn, phòng chống thiên tai, y tế, phòng chống dịch bệnh, một yêu cầu quan trọng nhất thường thấy là lực lượng cứu hộ, cứu nạn cần biết một người bị mất tích, bị nạn đang ở đâu. Nếu chúng ta nhận định người đó có mang theo một thiết bị di động thì việc tìm kiếm sẽ hiệu quả, nhanh chóng hơn nhiều khi định vị được máy di động đó.

Ví dụ điển hình trên thế giới chính là dịch vụ cứu hộ khẩn cấp 911 (hay E911) của Mỹ và Canada. Khi nhận được một cuộc gọi điện thoại khẩn cấp, hệ thống E911 sẽ tự động tính toán và xác định cho nhà chức trách biết vị trí của người gọi, để họ cử lực lượng hỗ trợ đến đó. Theo thống kê, E911 phục vụ được đến 96% lãnh thổ Mỹ. Như vậy, ở các nơi không có máy điện thoại cố định thì phải dùng định vị di động (tức là đa phần người gọi khẩn cấp gọi bằng máy di động).

- Đối với an ninh công cộng, một trong những yêu cầu thường xuyên và quan trọng nhất là cần biết một đối tượng, mục tiêu đang ở đâu, đi đâu. Có nhiều cách để biết các thông tin trên, tuy nhiên, chúng ta có thể thấy bằng cách định vị, theo vết một số thuê bao, một máy điện thoại di động mà đối tượng đó sử dụng hoặc mang theo là hiệu quả.

Những ứng dụng trên được tổng hợp từ các tài liệu tham khảo về kỹ thuật định vị di động, thông tin khoa học và thực tế.

Trên phương diện ứng dụng tổng quát, bài toán định vị di động hiện nay có thể phân chia làm các dạng sau:

- Một là dạng chủ động như đối với nhà cung cấp dịch vụ di động, họ có số liệu và sẽ tự tính toán để biết được vị trí của thuê bao, máy di động mà họ cần kết nối và cung cấp dịch vụ.

- Hai là dạng bị động như đối với doanh nghiệp kinh doanh, đơn giản họ chỉ cần có được vị trí GPS (nằm trong máy điện thoại) của khách hàng, đối tượng đang phục vụ và "hỏi" nhà mạng di động rằng vị trí ở đâu. Hoặc chính nhà mạng sẽ cung cấp dịch vụ vị trí đó cho doanh nghiệp.

- Ba là dạng bán chủ động như đối với cơ quan cứu hộ khẩn cấp như E911, đơn giản là họ có hệ thống kỹ thuật kết nối với các nhà mạng, và sử dụng hệ thống tự động nhận dạng vị trí (ALI) xác định vị trí người gọi và định vị nó trên bản đồ số.

- Bốn là, dạng hỗn hợp như đối với an ninh công cộng, do đặc điểm kỹ thuật định vị di động và tính chất sử dụng đa dạng, để xác định được vị trí của một đối tượng, mục tiêu hay một thiết bị di động, họ phải dùng nhiều phương pháp, cả chủ động, bị động, bán chủ động nêu trên hoặc kết hợp nhiều phương pháp cùng lúc.

1.2. Những giả thuyết, lý giải trước đây về định vị di động và ứng dụng cho công tác an ninh

1.2.1. Cơ sở lý thuyết liên quan

Cơ sở lý thuyết, nguyên lý kỹ thuật liên quan đến nội dung đề tài luận án cần nghiên cứu như sau:

(1) Nguyên lý kỹ thuật định vị di động.

(2) Lý thuyết phân lớp, xác định đối tượng; các phương pháp thu thập dữ liệu định vị; giải pháp cải thiện độ chính xác định vị; phương pháp bảo mật thông tin chuyển giao kết quả định vị; kỹ thuật giả lập trạm gốc thu thập tham số IMSI/IMEI.

Trong đó, các nguyên lý kỹ thuật định vị di động được trình bày cụ thể sau đây để làm cơ sở cho các nghiên cứu tiếp theo của luận án. Các cơ sở khoa học và kỹ thuật liên quan khác sẽ được trình bày trong các chương sau.

1.2.2. Nguyên lý kỹ thuật định vị di động

1.2.2.1. Khái quát

Định vị di động có thể thực hiện bởi một số nguyên lý kỹ thuật, chẳng hạn như kỹ thuật tìm điểm giao thoa tín hiệu vô tuyến giữa (một số) tháp thu phát sóng di động của mạng và máy điện thoại hoặc đơn giản bằng cách sử dụng dữ liệu của hệ thống vệ tinh dẫn đường toàn cầu GNSS [23].

Để định vị điện thoại di động bằng cách tìm điểm giao thoa tín hiệu vô tuyến di động, điện thoại đó phải phát ra ít nhất tín hiệu nhàn rỗi (tín hiệu chờ - Idle) để liên lạc với các cột ăng ten gần đó và không yêu cầu kích hoạt một cuộc gọi. Hệ thống điện thoại di động toàn cầu GSM thực hiện kết nối điện thoại di động với mạng dựa trên cường độ tín hiệu của điện thoại tới các cột ăng ten gần đó [26].

Kỹ thuật định vị có thể được sử dụng cho các dịch vụ dựa trên vị trí (LBS) [30, 31] và khi đó sẽ tiết lộ tọa độ thực của điện thoại di động. Các công ty viễn thông di động sử dụng kỹ thuật này để xác định vị trí gần đúng của điện thoại di động và cả người dùng của nó.

1.2.2.2. Tổng quan các nguyên lý kỹ thuật định vị di động

Vị trí của thiết bị di động (điện thoại di động) có thể được xác định theo các nguyên lý kỹ thuật cụ thể sau đây [23 -33]:

a. Kỹ thuật định vị dựa trên mạng (Network-Based)

Vị trí của điện thoại di động có thể được xác định trên cơ sở hạ tầng mạng của nhà cung cấp dịch vụ. Ưu điểm của các kỹ thuật dựa trên mạng là chúng có thể được thực hiện mà không ảnh hưởng đến thiết bị cầm tay (tức không xâm phạm/ảnh hưởng đến người dùng). Các kỹ thuật dựa trên mạng đã được phát triển nhiều năm trước khi GPS trên thiết bị cầm tay được phổ biến rộng rãi.

Kỹ thuật định vị của một điện thoại di động dựa trên việc đo mức công suất và các phần tử ăng-ten, đồng thời sử dụng nguyên lý một điện thoại di động được cấp nguồn luôn giao tiếp vô tuyến với một trong những trạm gốc (BTS/eNB) gần nhất. Do đó, các hiểu biết về vị trí của trạm gốc gợi ý rằng điện thoại di động cần định vị đang ở gần trạm gốc đó.

Các hệ thống tiên tiến xác định khu vực mà điện thoại di động ở đó và ước tính gần đúng khoảng cách đến trạm gốc. Xác định khoảng cách gần đúng được tính toán bằng phép nội suy tín hiệu giữa các cột ăng ten liền kề. Các dịch vụ đủ tiêu chuẩn có thể đạt được độ chính xác đến 50 mét ở các khu vực đô thị nơi lưu lượng truy cập di động và mật độ các cột ăng ten (trạm gốc) đủ cao. Tại các khu vực nông thôn và hoang vắng, do các trạm gốc có thể cách nhau hàng km nên việc xác định vị trí của điện thoại di động sẽ kém chính xác hơn. Định vị GSM sử dụng kỹ thuật giao thoa tín hiệu vô tuyến để xác định vị trí của điện thoại di động GSM hoặc sử dụng thiết bị theo dõi chuyên dụng.

Độ chính xác của các kỹ thuật dựa trên mạng là khác nhau. Trong đó kỹ thuật dựa trên nhận dạng tế bào (Cell-ID) là kém chính xác nhất (do có tín hiệu can nhiễu chuyển đổi giữa các tháp di động, hay còn gọi là "tín hiệu phản xạ/dội ngược"); kỹ thuật đo tam giác có độ chính xác vừa phải và kỹ thuật đo tam giác tín hiệu đường lên tiên tiến bằng định thời gian là mới hơn và có độ chính xác cao nhất. Độ chính xác của các kỹ thuật dựa trên mạng đều phụ thuộc vào mật độ của các trạm gốc tế bào. Trong đó, môi trường đô thị thường đạt được độ chính xác cao nhất có thể do có số lượng tháp phát sóng nhiều hơn và sử dụng kỹ thuật định vị bằng phương pháp định thời gian tiên tiến nhất.

Một trong những thách thức chính của các kỹ thuật dựa trên mạng là yêu cầu sự hợp tác chặt chẽ với nhà cung cấp dịch vụ (nhà mạng), nó đòi hỏi phải lắp đặt phần cứng và cài đặt phần mềm trong cơ sở hạ tầng của nhà điều hành mạng di động. Thông thường, việc đặt phần cứng và phần mềm trong cơ sở hạ tầng của nhà mạng phải được pháp luật của nước đó cho phép. Chẳng hạn như qui định của Mỹ trong bộ luật cho dịch vụ cấp cứu, cứu hộ, cứu nạn E911 buộc nhà mạng di động phải triển khai giải pháp kỹ thuật cung cấp khả năng định vị cho E911 trước khi cung cấp dịch vụ di động [25].

b. Kỹ thuật định vị dựa trên thiết bị cầm tay (Handset Based)

Vị trí của điện thoại di động có thể được xác định bằng cách sử dụng phần mềm khách được cài đặt trên máy điện thoại cầm tay. Kỹ thuật này xác định vị trí của

thiết bị cầm tay bằng cách tính toán vị trí của tế bào di động và cường độ tín hiệu của các tế bào nhà và lân cận mà liên tục được gửi từ thiết bị cầm tay đến nhà cung cấp dịch vụ. Ngoài ra, nếu điện thoại cầm tay được trang bị GPS thì có thể lấy được thông tin vị trí chính xác hơn do vị trí GPS của máy cầm tay có thể được gửi đến nhà cung cấp dịch vụ. Một cách tiếp cận khác là sử dụng kỹ thuật dựa trên dấu vân tay, trong đó "chữ ký" của tế bào nhà và tế bào lân cận báo hiệu cường độ tín hiệu tại các điểm khác nhau trong khu vực quan tâm được ghi lại và khớp trong thời gian thực để xác định vị trí của thiết bị cầm tay. Kỹ thuật này thường được thực hiện độc lập với nhà cung cấp dịch vụ.

Nhược điểm chính của các kỹ thuật dựa trên thiết bị cầm tay là sự cần thiết phải cài đặt phần mềm trên thiết bị. Nó đòi hỏi sự hợp tác tích cực, chặt chẽ của người sử dụng thuê bao di động cũng như phần mềm cài đặt phải có khả năng xử lý các hệ điều hành khác nhau của thiết bị cầm tay mà nó liên tục được thay đổi. Nhưng điều này là khó khả thi vì đối tượng của CQAN thường là đối tượng giấu mặt, khó tiếp cận hoặc chúng ở nước ngoài. Thông thường, chẳng hạn như điện thoại thông minh sẽ có thể cài đặt và chạy phần mềm định vị đó cũng như cài đặt, chạy các phần mềm bản đồ số như Google Maps để phục vụ kỹ thuật định vị dựa trên máy cầm tay.

Một giải pháp được đề xuất là cài đặt phần cứng hoặc phần mềm nhúng trên thiết bị cầm tay, ví dụ phần mềm sử dụng kỹ thuật định vị bằng cách tính toán Chênh lệch thời gian quan sát nâng cao (E-OTD). Qua khảo sát, nghiên cứu, sẽ nhận thấy phương pháp này không đạt được bước tiến đáng kể, do khó có thể thuyết phục các nhà sản xuất điện thoại di động khác nhau hợp tác trên một cơ chế chung và chi phí sản xuất điện thoại di động sẽ tăng cao. Một khó khăn khác là phải giải quyết vấn đề kỹ thuật của các thiết bị cầm tay nước ngoài đang chuyển vùng trong mạng của nhà cung

c. Kỹ thuật định vị dựa trên SIM

Sử dụng mô-đun nhận dạng thuê bao di động (SIM) trong thiết bị cầm tay GSM và UMTS, có thể thu được các phép đo vô tuyến thô từ thiết bị cầm tay. Các phép đo khả dụng bao gồm: Cell-ID đang phục vụ, thời gian phản hồi và cường độ

tín hiệu. Loại thông tin thu được qua SIM có thể khác với loại thông tin có sẵn từ điện thoại. Ví dụ: có thể không trực tiếp lấy được bất kỳ phép đo thô nào từ thiết bị cầm tay nhưng vẫn nhận được các phép đo thông qua SIM.

d. Kỹ thuật định vị dựa trên Wi-Fi

Dữ liệu Wi-Fi từ nguồn dữ liệu Wifi cộng đồng cũng có thể được sử dụng để xác định vị trí của thiết bị cầm tay. Hiệu suất kém của các kỹ thuật định vị dựa trên GPS trong môi trường trong nhà (do tín hiệu thu GPS từ vệ tinh sẽ yếu, không đủ cả ba vệ tinh cần thiết hoặc không thể thu được khi thiết bị cầm tay có gắn GPS ở trong nhà) và sự phổ biến ngày càng tăng của Wi-Fi đã khuyến khích các viện nghiên cứu, các công ty thiết kế các phương pháp mới và khả thi để thực hiện định vị điện thoại di động hoặc thiết bị di động trong nhà dựa trên Wi-Fi.

Hầu hết các điện thoại thông minh đều tích hợp modul lấy dữ liệu từ Hệ thống vệ tinh dẫn đường toàn cầu (GNSS), chẳng hạn như GPS của Mỹ, GLONASS của Nga, Galileo của Châu Âu, Beidou của Trung Quốc với hệ thống định vị Wifi.

e. Nguyên lý kỹ thuật lai ghép (hỗn hợp)

Hệ thống định vị lai ghép sử dụng kết hợp các kỹ thuật dựa trên mạng và dựa trên thiết bị cầm tay để xác định vị trí. Một ví dụ là phương pháp sử dụng một số chế độ của GPS có hỗ trợ (A-GPS), có thể sử dụng cả dữ liệu GPS và thông tin mạng để tính toán vị trí của thiết bị cầm tay. Cả hai loại dữ liệu này đều được điện thoại sử dụng để làm cho vị trí chính xác hơn (tức là kỹ thuật A-GPS). Ngoài ra, kỹ thuật định vị lai ghép bằng cách theo dõi cả hai hệ thống cũng có thể thực hiện bằng cách để điện thoại thu được vị trí GPS của nó trực tiếp từ vệ tinh, sau đó nó gửi thông tin qua mạng tới người đang muốn xác định vị trí của điện thoại.

Các hệ thống sử dụng kỹ thuật định vị lai ghép điển hình bao gồm: dịch vụ định vị của Google Maps, kỹ thuật OTDoA và E-CellID của mạng 4G-LTE. Ngoài ra còn có các hệ thống định vị kết hợp một số phương pháp tiếp cận/xác định vị trí khác nhau để định vị thiết bị di động bằng Wi-Fi, WiMAX, GSM, 4G-LTE, địa chỉ IP và dữ liệu môi trường mạng, trong đó có dữ liệu đa phương tiện mà thiết bị di động đã và đang sử dụng trên môi trường mạng đó.

Phương pháp định vị này có thể được gọi là phương pháp lai ghép tiên tiến, nó kết hợp được cả các dịch vụ định vị dựa trên vị trí thông thường (LBS) và dịch vụ định vị dựa trên đa phương tiện của vị trí (LBM).

g. Tổng hợp các kỹ thuật định vị

Trong bảng dưới đây, luận án tổng hợp một số nguyên lý kỹ thuật, thuật toán định vị khả dụng làm cơ sở tính toán, lựa chọn giải pháp kỹ thuật định vị theo mục tiêu đặt ra. Bảng tổng hợp này được tham khảo từ các nguồn tài liệu [23-45].

Bảng 1. 1. Tổng hợp các kỹ thuật định vị di động

TT	Kỹ thuật	Mô tả/Định nghĩa/Khái niệm	Thuật toán/ Công thức tính toán cơ bản
I	**Dựa trên mạng**	Định vị dựa trên thông tin tính toán của mạng di động	
1	Multilateration (MLAT)	Kỹ thuật đo đa phương hay còn gọi là kỹ thuật định vị hyperbolic, là kỹ thuật tính toán vị trí của thiết bị trên cơ sở đo thời gian đến (ToA) thiết bị của sóng vô tuyến được phát từ nhiều trạm gốc. Do đã biết dạng sóng, tốc độ và địa điểm các trạm gốc, nên sẽ tính được vị trí của thiết bị cần định vị.	ToAs (thời điểm đến) = ToFs (thời gian bay) + ToT (thời điểm phát).
2	Triangulation	Kỹ thuật đo tam giác để tính toán vị trí của thiết bị bằng cách vẽ các đường cắt thành hình tam giác từ các điểm phát sóng đã biết (các BTS/eNB) đến thiết bị (còn gọi là kỹ thuật đo tam giác đường xuống tiên tiến).	Các thuật toán tính toán tam giác đạc.
II	**Dựa trên máy cầm tay**	Định vị dựa trên phần mềm khách cài đặt trên máy cầm tay, ví dụ phần mềm ứng dụng vị trí GPS trên máy điện thoại thông minh. Kỹ thuật này xác định vị trí của thiết bị cầm tay bởi các tham số nhận dạng tế bào Cell-ID của mạng di động phục vụ nó, cường độ tín hiệu của các tế bào nhà và lân cận, liên tục được gửi đến nhà cung cấp dịch vụ.	- Các thuật toán tính toán tọa độ địa lý trên cơ sở tín hiệu GPS từ vệ tinh đến máy cầm tay. - Thuật toán tính chênh lệch thời gian quan sát nâng cao E-OTD. Thuật toán tính chênh lệch thời gian đến của đường lên U-TDoA.

TT	Kỹ thuật	Mô tả/Định nghĩa/Khái niệm	Thuật toán/ Công thức tính toán cơ bản
		Một cách tiếp cận khác là dựa trên "dấu vân tay", trong đó "chữ ký" của Cell nhà và Cell lân cận báo hiệu cường độ tín hiệu tại điểm quan tâm khác nhau, được ghi lại và khớp với thời gian thực để tính toán vị trí của máy cầm tay. (Phương pháp này độc lập với nhà cung cấp dịch vụ, thường được sử dụng trong các thiết bị định vị cơ động).	
III	**Dựa trên SIM**	Đo các tham số vô tuyến từ máy cầm tay bằng cách sử dụng SIM của nó. Các tham số đo được là Cell-ID đang phục vụ, thời gian phản hồi và cường độ tín hiệu. Từ đó tính toán được vị trí của máy cầm tay.	Các thuật toán tính toán giữa tham số Cell, thời gian phản hồi và cường độ tín hiệu.
IV	**Dựa trên Wifi**	Xác định vị trí của thiết bị cầm tay bằng cách lấy dữ liệu Wi-Fi nguồn cộng đồng	
1	Signal strength based (AP-RSSI)	Kỹ thuật ghi lại cường độ tín hiệu RSSI từ một số điểm truy cập trong phạm vi máy cầm tay để tính toán vị trí máy cầm tay.	Sử dụng các thuật toán đo tam giác như mô tả ở trên.
2	Fingerprinting based	Kỹ thuật ghi lại cường độ tín hiệu RSSI từ một số điểm truy cập vào cơ sở dữ liệu, lấy một tọa độ đã biết của thiết bị khách trong giai đoạn ngoại tuyến, ước tính được vị trí gần đúng nhất khi nó trực tuyến.	Các thuật toán đo tam giác và các thuật toán ước lượng.
3	Angle of arrival based (AoA)	Kỹ thuật ước tính góc đến (AoA) của tín hiệu đa đường nhận được tại các mảng ăng-ten trong các điểm truy cập và áp dụng phương pháp đo tam giác để tính toán vị trí của các thiết bị khách.	Thuật toán Music.

TT	Kỹ thuật	Mô tả/Định nghĩa/Khái niệm	Thuật toán/ Công thức tính toán cơ bản
4	Time of flight based (ToF)	Kỹ thuật lấy dấu thời gian được cung cấp bởi các giao diện không dây để tính toán ToF của tín hiệu và sau đó sử dụng thông tin này để ước tính khoảng cách và vị trí tương đối của một thiết bị khách đối với các điểm truy cập.	- Thuật toán đo tam giác - Thuật toán đo thời gian
V	**Lai ghép tiên tiến**		
1	A-GNSS (A-GPS)	Kỹ thuật định vị toàn cầu có hỗ trợ, để tính toán vị trí máy cầm tay từ cả thông tin tọa độ GPS và thông tin mạng (điện thoại có được vị trí GPS của nó trực tiếp từ vệ tinh và sau đó gửi thông tin qua mạng tới người đang định vị điện thoại đó).	-Thuật toán của Google Maps. -Thuật toán OTDoA và E-CellID của mạng 4G LTE.
2	Kết hợp	Kỹ thuật kết hợp một số phương pháp tiếp cận vị trí khác nhau để định vị thiết bị di động bằng Wi-Fi , WiMAX , GSM, LTE, địa chỉ IP và dữ liệu môi trường mạng.	Nhiều thuật toán của các kỹ thuật trên kết hợp với nhau để định vị hoặc dùng mỗi thuật toán tùy theo dữ liệu vào khả dụng.

1.2.3. So sánh các công nghệ định vị di động

Như đã phân tích ở trên, có nhiều nguyên lý kỹ thuật định vị di động, trong đó có hai loại chính: kỹ thuật định vị dựa trên mạng và kỹ thuật định vị dựa trên thiết bị cầm tay. Nội dung sau đây tiến hành so sánh hai công nghệ sử dụng hai nguyên lý kỹ thuật này bằng các tiêu chí cơ bản gồm: độ chính xác, độ tin cậy, tính khả dụng, độ trễ, khả năng áp dụng cũng như cách áp dụng các kỹ thuật định vị.

1.2.3.1. Mô tả công nghệ cần so sánh

Để so sánh, phần sau đây tiến hành phân tích sâu hơn về nguyên lý kỹ thuật của hai công nghệ định vị dựa trên mạng và dựa trên thiết bị cầm tay.

a. Công nghệ định vị di động dựa trên mạng

Công nghệ này được gọi là "dựa trên mạng" vì sử dụng mạng, cùng với thiết bị chuyên dụng xác định vị trí trên cơ sở mạng được sử dụng để định vị thiết bị di động.

Đó là các phương pháp đo Đa phương (đo nhiều BTS/eNB đồng thời), Đơn phương (một MS/UE đo nhiều BTS/eNB) và ví dụ là các phương pháp đo Góc tín hiệu đến (AoA) và đo Thời gian đến (ToA)/ đo Chênh lệch thời gian đến (TDoA), rộng hơn là đo Chệch lệch thời gian đến của đường lên (U-TDoA) hay đo Chênh lệch thời gian đến của đường xuống (OTDoA). Phương pháp đo Song phương (chỉ một MS/UE hoặc BTS/eNB) là điển hình của kỹ thuật tính toán Cell-ID, Cell – ID + Chênh lệch thời gian khứ hồi (RTD) và Lấy dấu vân tay vị trí (LF). Điều đáng chú ý là, trong mạng GSM, RTD được gọi là định thời tiên tiến (TA) và trong hệ thống mạng 3G, 4G, được gọi là Độ trễ khứ hồi (RTT).

Ngoài ra, phương pháp LF, được giải thích ngắn gọn là: "Kỹ thuật LF" sử dụng các mẫu sóng cao tần RF ở xa (đặc tính pha và biên độ đa đường) của tín hiệu vô tuyến đến ăng-ten máy thu từ một người gọi. Các đặc điểm độc đáo của tín hiệu, bao gồm cả dạng đa đường của nó được phân tích và "dấu vân tay" được xác định cho một khu vực xác định. Sau đó, "dấu vân tay" được so sánh trong cơ sở dữ liệu. Bằng cách đối sánh dấu vân tay của tín hiệu người gọi với cơ sở dữ liệu về dấu vân tay đã biết, vị trí địa lý của người gọi được xác định cho một trong các khu vực được khảo sát.

b. Công nghệ định vị di động dựa trên thiết bị cầm tay

Công nghệ này được gọi là "dựa trên thiết bị cầm tay" vì bản thân thiết bị cầm tay (MS/UE) là phương tiện chính để mạng định vị người dùng, mặc dù mạng có thể sử dụng để hỗ trợ việc xác định thiết bị di động và/ hoặc đưa ra ước tính vị trí dựa trên dữ liệu đo lường và các thuật toán xác định vị trí dựa trên máy cầm tay.

Ở đây MS/UE có một phần tích cực trong việc đo vị trí (đơn phương), nhưng tính toán vị trí là ở phần cuối của mạng. Trong mạng GSM, phương pháp đơn phương này được gọi là Chênh lệch thời gian quan sát nâng cao (EOTD); trong mạng CDMA Mỹ, được gọi là Phương pháp đo tam giác Liên kết Chuyển tiếp Nâng cao (AFLT); và trong các hệ thống 3G/4G, phương pháp tương tự này được gọi là Chênh lệch Thời gian Đến của Đường xuống - Quan sát Thời gian Không hoạt động (IPDL-OTDoA). Tuy nhiên, việc thực hiện định vị hoàn

toàn dựa trên thiết bị cầm tay là không hiệu quả vì kích thước bộ nhớ nhỏ của ứng dụng khách LCS (bộ nhớ ít hơn đồng nghĩa với độ trễ nhiều hơn) và thời lượng pin thường ít, không đủ cho xử lý định vị.

Bảng dưới đây phân loại các kỹ thuật định vị di động đã phân tích ở trên.

Bảng 1. 2. Phân loại các kỹ thuật định vị di động

Loại 1 / **Loại 2**	**Kỹ thuật dựa trên máy cầm tay (Handset – Based)**	**Kỹ thuật dựa trên mạng (Network – Based)**	
	Dựa trên MS được mạng hỗ trợ	Dựa trên mạng được hỗ trợ	Dựa trên mạng đơn giản
Đa phương	Không	Không	AoA, ToA hoặc TDoA
Đơn phương	EOTD, AFLT, OTDoA, Rx-Level	EOTD, AFLT, IPDL, OTDoA, Rx-Level	Rx-Level (Mức vô tuyến)
Song phương	Cell Convegare (vùng phủ của Cell), CI+RTD	Không	LF, Cell Convegare (vùng phủ của Cell), CI+RTD

Lưu ý rằng một số phương pháp định vị có thể thuộc cả hai loại (lai ghép/ kết hợp cả hai loại) tùy thuộc vào cách tiếp cận triển khai. Ví dụ kỹ thuật EOTD trong đó máy thu thực hiện các phép đo TDoA và gửi chúng trở lại mạng để tính toán vị trí (do MS/UE hỗ trợ) hoặc tự tính toán vị trí (dựa trên MS/UE).

1.2.3.2. Thực hiện so sánh

Trong phần này, ta sẽ xác định và xem xét chi tiết từng tiêu chí để đánh giá và so sánh hai công nghệ định vị nêu trên.

a. Độ chính xác

Độ chính xác của công nghệ định vị là một thước đo xác định *mức độ gần của các phép đo vị trí với vị trí thực tế của máy di động* đang được định vị. Về cơ bản, vị trí đo càng gần với vị trí thực thì kết quả đo càng chính xác. Khi đánh giá độ chính xác của thiết bị định vị, người ta thường xem xét có bao nhiêu phép đo vị trí được thực hiện, cách tính điểm các phép đo vị trí và kết quả được trình bày dưới dạng nào. Một hàm điểm được sử dụng rộng rãi trong đánh giá độ chính xác của nhiều phép đo vị trí là căn bậc hai

của sai số bình phương trung bình (RMSE), trong đó RMSE được đưa ra bởi công thức sau:

$$\text{RMSE} = \sqrt{\frac{1}{n}\sum_{k=1}^{n}(x_{mesuredk} - x_{true})^2} \quad (1.1)$$

Trong đó n là số phép đo trong tập hợp và k là chỉ số của phép đo. Bộ này có thể chứa tất cả các phép đo vị trí đã thử hoặc chỉ các phép đo thành công và trong mỗi trường hợp, được sử dụng để đánh giá độ chính xác của phương pháp định vị. Nếu chỉ vị trí thành công được sử dụng, tỷ lệ của các phép đo vị trí thành công trong số tất cả các phép đo vị trí đã thử có thể được báo cáo riêng (tỷ lệ này được gọi là độ tin cậy và được xem xét trong phần tiếp theo).

Giá trị của hàm điểm được sử dụng để đánh giá độ chính xác hai hoặc ba chiều. Độ chính xác hai chiều (trong đó độ cao bị bỏ qua) chủ yếu được sử dụng trong định vị di động. Nó thường được gọi là độ chính xác ngang được nêu là *2drms* nếu sử dụng điểm RMSE. Độ chính xác một chiều là độ lệch đo dọc theo độ cao hoặc độ chính xác xuyên tâm, là độ lệch đo trong khoảng cách từ vị trí thực đến vị trí được đo.

Các phương pháp phổ biến khác để tính độ chính xác là dựa trên phép tính xác suất cổ điển. Ở đây, xác suất của nhiều phép đo vị trí nằm trong một bán kính hoặc hình cầu nhất định được báo cáo để minh họa sự phân bố của các phép đo vị trí. Nói chung, không có kiến thức về các thuộc tính thống kê của các phép đo vị trí, chúng ta chỉ sử dụng Xác suất Sai số Hình tròn (CERP) cho các trường hợp 2 chiều và Xác suất Sai số Hình cầu (SERP) cho các trường hợp 3 chiều. CERP là đơn vị được sử dụng rộng rãi nhất. Ví dụ, 95% CERP trong vòng 50 mét có nghĩa là 95% các phép đo vị trí nằm trong vòng 50m tính từ vị trí thực. Xác suất lỗi cũng có thể được sử dụng để đặt giới hạn cho độ chính xác tối đa cho phép đo.

Ví dụ: các yêu cầu của FCC liên quan đến các cuộc gọi khẩn cấp 911 ở Mỹ với độ chính xác định vị là 67% và 95% CERPs, như bảng 1.3.

Bảng 1. 3. Yêu cầu độ chính xác của dịch vụ cứu hộ FCC-911 ở Mỹ

Phương pháp	67% CERP (m)	95% CERP (m)	Chú thích
Dựa trên máy cầm tay	50	150	Ví dụ GPS
Dựa trên mạng	100	300	Ví dụ ToA, không có khả năng định vị trong máy cầm tay
Giải pháp phần mềm mạng (NSS)	1000	không	1) Ví dụ CI+TA 2) Độ chính xác bán kính
EOTD (1) EOTD (2)	100 50	300 150	1) Thử trong tháng 10/2001 2) Thử trong và sau 1/10/2003.

Mức độ chính xác cho các ứng dụng nhận biết vị trí có thể được phân loại theo bảng 1.4.

Bảng 1. 4. Mức độ chính xác của các dịch vụ dựa trên vị trí

Độ chính xác	Biên độ
Thấp	Lớn hơn 150m
Trung bình	50 đến 150 m
Cao	Nhỏ hơn 50m

b. Độ tin cậy

Nói chung, một phép đo thống nhất về độ tin cậy rất khó xác định do sự khác nhau của công nghệ. Trong hệ thống GPS, độ tin cậy được định nghĩa là thước đo mức độ nhất quán của mức sai số ngang GPS có thể được duy trì dưới ngưỡng độ tin cậy qui định. Trong các phương pháp định vị di động, chúng ta có thể định nghĩa một cách đơn giản về độ tin cậy như sau: *Độ tin cậy là tỷ lệ số lần định vị thành công trong số tất cả các lần thử định vị được thực hiện.*

Các hệ thống được sử dụng trong định vị cá nhân phải cung cấp hiệu suất cực kỳ đáng tin cậy, đặc biệt là trong các trường hợp khẩn cấp vì hỏng hóc có thể rất bất lợi. Theo quan điểm khả năng sử dụng, các thiết bị định vị thường xuyên bị lỗi hoặc sai vị trí sẽ không đáng tin cậy. Do đó, cùng với độ chính xác, điều quan trọng không kém là biết mức độ đáng tin cậy của một công nghệ. Ở đây, các mức độ tin cậy cho các ứng dụng nhận biết vị trí khác nhau có thể được phân loại như trong bảng 1.2 đã nêu ở trên.

c. Độ trễ

Đo độ trễ về cơ bản là đo thời gian từ khi khởi động đến khi có được phép đo vị trí đầu tiên. Trong GPS, đây được gọi là thời gian sửa lỗi đầu tiên (TTFF). Yêu cầu cao về độ trễ thấp hoặc ngắn không chỉ được thực hiện trong các trường hợp khẩn cấp mà còn theo quan điểm của LBS. Ví dụ, QoS và khả năng sử dụng của các ứng dụng hướng dẫn và theo dõi giảm nếu một ứng dụng không thể đảm bảo hoạt động theo thời gian thực. Độ trễ ngắn cũng giúp tiết kiệm điện năng. Nó được đo bằng giây. Độ trễ tiếp tục được chia thành ba thành phần là độ trễ thiết lập cuộc gọi, độ trễ mạng và độ trễ xử lý.

Nói một cách khác, độ trễ thiết lập cuộc gọi là thời gian trôi qua từ khi bắt đầu cuộc gọi tại MS/UE đến khi nhận được phản hồi đầu tiên từ mạng. Độ trễ mạng được định nghĩa là thời gian cần thiết để truyền tất cả các tin nhắn không bao gồm độ trễ thiết lập cuộc gọi. Độ trễ xử lý, như tên của nó là thời gian cần thiết của thiết bị định vị để đo và tính toán vị trí.

d. Độ khả dụng

Tính khả dụng như một thước đo hiệu suất trong công nghệ định vị di động. Định nghĩa tính khả dụng bao gồm khái niệm về phạm vi và dung lượng, sẽ được nêu ở phần sau. Trên thực tế, tính khả dụng (sẵn có) phải là một thước đo của chính nó vì nó đo các khía cạnh khác nhau của vị trí so với độ chính xác và độ tin cậy, nó được minh họa theo hai điểm sau:

(1) Nếu điện thoại được trang bị GPS độc lập được đặt sâu dưới lòng đất, tín hiệu GPS không thể xuyên qua các bức tường dày và do đó tín hiệu bị chặn. Đương nhiên, tính năng định vị dựa trên GPS không thể thực hiện được tại thời điểm này. Ở đây, thực tế là tín hiệu bị chặn không có nghĩa là GPS không tốt về độ chính xác và độ tin cậy, mà nó không có khả năng sử dụng trong lòng đất.

(2) Xem xét một phương pháp dựa trên mạng di động, khả năng định vị tốt là do quy hoạch mạng cẩn thận hơn là hệ quả của các hiện tượng ngẫu nhiên ảnh hưởng đến các thiết bị đo vị trí và đường truyền tín hiệu. Nếu các trạm gốc hoặc trong trường hợp này là các vị trí đo được triển khai hiệu quả, thì tính sẵn sàng cho định vị có thể rất tốt tại khu vực đó.

Điều này gây khó khăn cho việc chính thức hóa một phép đo chung về tính khả dụng. Trong các phương pháp định vị dựa trên mạng di động, các yếu tố như dung lượng kênh, vùng phủ sóng, hình dạng trạm gốc và môi trường truyền tín hiệu ảnh hưởng đến tính khả dụng của vị trí.

Từ các thử nghiệm, báo cáo và mô phỏng đã công bố, các hạn chế về phạm vi phủ sóng, hình học và môi trường tín hiệu liên quan đến tính khả dụng định vị đã được nghiên cứu và được liệt kê trong bảng 1.5.

Bảng 1. 5. Phân loại tính khả dụng kém

Loại	Ví dụ tính khả dụng kém
Vùng xa xôi	Biển mở, sa mạc, vùng cực, và các khu vực không có Cell phủ sóng
Nông thôn	Bên cạnh làng mạc, các khu nhà ở, đường cao tốc
Thành thị nhỏ	Các khu nhà ở, khu tập thể, công viên, chợ, khu mua sắm, khu có tán lá cây rậm rạp
Thành thị	Khu nhà cao tầng và các cấu trúc cao, ngõ hẻm

Loại	Ví dụ tính khả dụng kém
Trong nhà	Trần thép, gỗ hoặc tường bê tông, các toà nhà thương mại
Dưới đất (ngầm)	Các hầm của các toà nhà, hầm để xe bằng bê tông

e. Khả năng ứng dụng

Về cơ bản, khả năng ứng dụng của định vị cho biết những hạn chế và yêu cầu vật lý liên quan đến việc triển khai và sử dụng công nghệ nhất định, cả về các vấn đề kỹ thuật và tài chính. Các vấn đề chính ảnh hưởng đến khả năng ứng dụng của các phương pháp định vị di động là tiêu thụ điện năng, kích thước phần cứng, độ phức tạp tính toán của phần mềm, tải xử lý, các chế độ định vị được hỗ trợ, sự phụ thuộc vào mạng, tải tín hiệu, chi phí và tiêu chuẩn hóa. Cụ thể như sau:

(1) Mức tiêu thụ nguồn:

Đây trở thành một yếu tố hạn chế nếu một phương pháp định vị đang sử dụng tài nguyên bên trong thiết bị cầm tay chỉ cho nhu cầu định vị hoặc nếu phần cứng chuyên dụng phải chạy để thực hiện các phép đo vị trí. Tại đây, các ước tính về mức tiêu thụ điện năng có thể được thực hiện trên cơ sở bảng dữ liệu và thông số kỹ thuật.

(2) Kích thước phần cứng:

Nếu cần các thành phần phần cứng bổ sung để định vị, thì kích thước vật lý cần thiết để chứa và/ hoặc tích hợp các thành phần này bên trong thiết bị cầm tay sẽ trở thành một vấn đề quan trọng. Mặc dù ngày càng có nhiều ứng dụng mới và đa phương tiện trên thiết bị cầm tay nhưng người dùng vẫn mong muốn kích thước thiết bị của họ ngày càng nhỏ hơn, do đó việc tăng kích thước thiết bị cầm tay vì khả năng định vị sẽ không đi kèm với mong muốn của người dùng.

(3) Kích thước phần mềm:

Một số phương pháp định vị yêu cầu phần mềm bổ sung để thực hiện các phép đo và/ hoặc tính toán vị trí hoặc để hỗ trợ định vị. Nếu yêu cầu phần mềm bổ sung, các giới hạn thực tế có thể liên quan đến kích thước của phần mềm do bộ nhớ hoặc các tài nguyên khác có sẵn trong thiết bị di động bị hạn chế.

(4) Xử lý tải:

Đối với các ứng dụng thời gian thực, việc cung cấp đủ tải xử lý là điều bắt buộc, nhưng nhu cầu về bộ xử lý bổ sung trở thành một vấn đề khó khăn trong bối cảnh yêu cầu kích thước ngày càng giảm của các thiết bị cầm tay.

(5) Chế độ định vị được hỗ trợ:

Các phép đo vị trí có thể là một giải pháp điểm hoặc một giải pháp liên tục hoặc được lọc. Trong giải pháp điểm, chỉ cần một tập hợp các phép đo để thực hiện công việc, ví dụ như định vị chỉ khi có các cuộc gọi. Ngược lại, trong giải pháp được lọc, chẳng hạn như ứng dụng điều hướng hoặc hướng dẫn yêu cầu định vị liên tục.

Do đó, các chế độ được hỗ trợ có tác động lớn đến khả năng ứng dụng, tức là, tùy thuộc vào công nghệ định vị, một hoặc cả hai chế độ được hỗ trợ.

(6) Tải trọng mạng và tín hiệu phụ thuộc:

Nếu một phương pháp định vị chỉ phụ thuộc vào một mạng để hỗ trợ phép đo và định vị, thì khả năng sử dụng chung của nó trong các ứng dụng thiên về định vị sẽ bị giảm.

Tải tín hiệu sẽ trở thành một yếu tố hạn chế nếu một phương pháp định vị yêu cầu giao tiếp hai chiều chuyên sâu giữa phần tử mạng và máy di động hoặc một lượng lớn dữ liệu hỗ trợ với thông báo rất ngắn. Do đó nên ước tính tải tín hiệu dự kiến trung bình và tối đa nếu phương pháp định vị phụ thuộc vào mạng.

(7) Chi phí:

Mặc dù có hiệu suất tốt, một phương pháp định vị có thể không được áp dụng nếu chi phí triển khai và hoạt động của nó rất cao so với một số phương pháp khác, mặc dù nó có thể không có cùng mức hiệu suất và công

nghệ. Đối với điện thoại di động, chi phí thiết bị cầm tay được giảm thiểu nếu một phương pháp định vị là áp dụng trực tiếp cho tất cả các thế hệ điện thoại bao gồm cả điện thoại thế hệ đã cũ (điện thoại đang dùng).

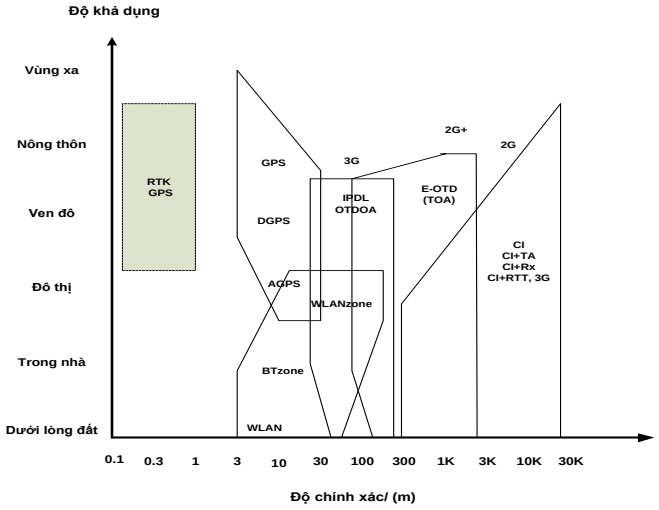
(8) Tiêu chuẩn hóa:

Cuối cùng, tiêu chuẩn chung là yếu tố sống còn, là vấn đề khả năng áp dụng công nghệ định vị. Tiêu chuẩn chung được đặt ra có một vai trò quan trọng trong phát triển và triển khai các công nghệ định vị. Để có tiêu chuẩn chung, cần phải thực hiện chuẩn hóa giao diện để cho phép chuyển vùng và tương tác giữa thiết bị đầu cuối và mạng từ các nhà cung cấp khác nhau đang được tiến hành. Quá trình hợp tác này đã được các nhà cung cấp nền tảng mạng di động trên thế giới thực hiện.

Như vậy, rất khó có thể xác định một phép đo chung cho khả năng áp dụng công nghệ định vị di động nào cho bài toán thực tế của đề tài luận án đặt ra. Tuy nhiên, rất khả thi là có nhiều công nghệ và ứng dụng định vị, ta sẽ tùy theo yêu cầu mà lựa chọn một trong các công nghệ hoặc hỗn hợp (lai ghép) các công nghệ định vị để đạt các tính năng, tiêu chí cần thiết từ thấp, trung bình đến cao.

g. So sánh chung giữa các công nghệ định vị

Hình sau đây là so sánh chung về độ chính xác và độ khả dụng của các công nghệ định vị khác nhau.



Hình 1. 1. So sánh độ chính xác và độ khả dụng của các công nghệ định vị trong môi trường 2G, 2.5G, 3G

Ví dụ:

Sử dụng kỹ thuật E-OTD cho việc định vị một máy di động thế hệ 2G, độ chính xác tốt nhất cao hơn 100m một chút và trong trường hợp xấu hơn là trên 2km nhưng chưa đến 3km. Độ chính xác sẽ tăng dần đến dưới 100m khi ta di chuyển từ mặt đất vào trong nhà. Độ chính xác ít thay đổi khi di chuyển từ trong nhà ra khu vực thành phố và ngoại ô. Nhưng độ chính xác sẽ kém đi nếu đến những vùng nông thôn.

Bảng 1.6 so sánh các phương pháp định vị về độ trễ, độ tin cậy và tính khả dụng.

Bảng 1. 6. So sánh về độ trễ, độ tin cậy và tính khả dụng của các phương pháp định vị

Phương pháp định vị	Độ tin cậy	Độ trễ	Khả năng áp dụng
GPS			
Chỉ GPS	Cao	<35s	Cao
GPS được hỗ trợ (AGPS)	Trung bình	1-10s (ngoài trời)	Trung bình
Mạng di động			
AoA	Trung bình	Xấp xỉ 10s	Thấp
RSSI	Cao	<5s	Cao
LF	Thấp	<10s	Thấp
CI+TA	Cao	<5s	Cao
ToA/TDoA	Trung bình	<10s	Thấp
EOTD hoặc OTDoA-IPDL	Trung bình	<10s	Trung bình

Ta thấy, độ chính xác kém đi từ khoảng cách 100m đến 500m và trong trường hợp xấu hơn nó vẫn ở khoảng 2-3 km. Có thể thấy rằng phương pháp A-GPS là khả dụng nhất, nó có độ chính xác vượt trội so với các phương pháp khác, ngoại trừ trong nhà hoặc dưới lòng đất do khi đó sẽ mất hoặc có tín hiệu vệ tinh GPS kém [23 -45].

1.3. Các yêu cầu định vị di động của công tác an ninh

Định vị di động là một yêu cầu quan trọng của CQAN để truy tìm đối tượng cũng như tìm kiếm, cứu hộ, cứu nạn. Vậy cách mà CQAN tìm kiếm, xác định, định vị, truy vết được đối tượng đó như thế nào trên cơ sở bài toán định vị di động? Khi có tình huống khẩn cấp cần giúp đỡ, cứu hộ, cứu nạn, có nhu cầu cần thiết phải làm rõ, trả lời nhiều câu hỏi liên quan. Trong đó, các câu hỏi ai, ở đâu, đi đâu là cần thiết

đầu tiên và quan trọng nhất. Có nhiều cách để truy tìm, xác định được rằng đối tượng, mục tiêu đó ở đâu. Tuy nhiên, tất cả các cách đó đều hết sức khó khăn, phức tạp, kéo dài và đôi khi không tìm được.

Trong điều kiện thực tế hiện nay, hầu hết con người trong xã hội đã, đang và sẽ dùng hai hình thức liên lạc phổ biến với xã hội là thông qua mạng Internet và mạng di động. Trong đó, liên lạc qua mạng di động là phổ biến, vì từ khi có điện thoại di động thế hệ thứ 3, 4 trở lên, nó vừa có thể thực hiện các liên lạc truyền thống (nghe, gọi điện thoại, nhắn tin) vừa kết nối với mạng Internet để thực hiện các truy cập Internet, mạng xã hội, các dịch vụ liên lạc dựa trên mạng.

Do vậy, để tìm kiếm một đối tượng hay một mục tiêu cứu hộ, cứu nạn, ngoài các phương pháp thông thường, CQAN hoặc cơ quan cứu hộ có thể sử dụng kỹ thuật định vị thiết bị di động mà đối tượng, mục tiêu đó mang theo hoặc có thể mang theo.

Để định vị một đối tượng, trước hết ta phải biết đó có phải là đối tượng, mục tiêu cần tìm kiếm hay không. Tức là cần xác định nó có thuộc tập hợp các đối tượng đã được xác định hay không. Nếu có thì nó thuộc lớp nào trong các lớp đã được phân loại (phân hoạch) và cuối cùng xác định được đối tượng cụ thể. Nếu không thì ta phải thu thập dữ liệu đặc trưng và bổ sung vào cơ sở dữ liệu hiện có. Tiếp theo là xác định vị trí của đối tượng, tức là định vị. Chẳng hạn, khi cần tìm kiếm một đối tượng, mục tiêu, trước tiên cần tìm hiểu đối tượng đó là ai, có các đặc trưng, đặc điểm gì cùng các thông tin khác liên quan đến đối tượng. Tiếp đến họ cần tìm hiểu xem đối tượng có dùng điện thoại di động hay không (thuê bao hoặc sử dụng), xác minh và biết được số điện thoại mà họ có thể sử dụng, yêu cầu hỗ trợ tìm kiếm, định vị đối tượng, mục tiêu thông qua vị trí thuê bao đó xuất hiện. Câu hỏi tiếp theo là đối tượng đó "ở đâu" hoặc "đi đâu. Câu hỏi đó có thể là một phạm vi địa lý rất rộng cỡ quốc gia, vùng lãnh thổ hay một tỉnh, thành phố và hẹp hơn là một khu vực hoặc chính xác hơn là đến vị trí tọa độ địa lý hay địa chỉ nào đó.

Từ đây, luận án đề xuất đồng nhất khái niệm đối tượng, mục tiêu cần tìm kiếm với một thiết bị di động. Như phân tích từ đầu, đối với môi trường mạng 4G trở lên, có hỗ trợ truy cập Internet tốc độ cao thì đối tượng định vị đa dạng hơn một máy điện

thoại di động, mà là vị trí của một "thiết bị di động". Đối với thiết bị dạng máy tính của đối tượng mà truy cập trực tiếp Internet thì vùng ở đây có thể được định nghĩa là địa chỉ IP hoặc địa chỉ MAC. Đối với "thiết bị di động" nói chung hoặc loại có hỗ trợ 4G trở lên, thì còn thêm thông tin vùng gần hơn chính là Cell di động phục vụ. Nếu xác định được Cell di động phục vụ, thì ta đã khoanh được đối tượng ở một vùng hẹp tương đối, cỡ bán kính hàng trăm mét hoặc hàng km tùy khu vực thành thị, nông thôn.

Đến đây, bài toán đặt ra là phải xác định được ngày càng chính xác hơn vị trí của "thiết bị di động" mà đối tượng sử dụng, vị trí ở đây có thể là "ở đâu", tức là xác định địa điểm hay "đi đâu", tức là truy vết đường đi. Yêu cầu là tìm kiếm, xác định được vị trí càng chính xác càng tốt (cao nhất chính là tọa độ GPS, hay địa chỉ một ngôi nhà, căn nhà, căn phòng mà đối tượng xuất hiện).

1.4. Tình hình nghiên cứu liên quan, những tồn tại và hướng giải quyết

1.4.1. Tình hình nghiên cứu liên quan

1.4.1.1. Tài liệu tiếng Việt

Có một số nghiên cứu khoa học trong nước về định vị di động GSM (2G), định vị Wifi liên quan đến đề tài luận án như sau:

- Tác giả Lê Danh Cường, trong luận án tiến sĩ đã được bảo vệ thành công năm 2018, đã tiến hành nghiên cứu về một số nguyên lý kỹ thuật điển hình để định vị di động GSM (2G) qua giao diện vô tuyến; giải pháp bảo mật liên lạc GSM chuyên dùng bằng cách thiết lập trạm gốc di động dùng riêng. Nghiên cứu của TS. Lê Danh Cường đã giải quyết được cơ bản được về kỹ thuật định vị di động thế hệ 2G qua giao diện vô tuyến, giải pháp sử dụng trạm gốc dùng riêng thiết lập mạng liên lạc 2G chuyên dùng, bảo mật. Tuy nhiên, đề tài của TS. Lê Danh Cường chưa nghiên cứu về định vị di động 4G ứng dụng cho công tác an ninh [3].

- Tiến sĩ Vũ Trung Kiên, trong luận án tiến sĩ đã được bảo vệ thành công năm 2019, tiến hành nghiên cứu về nguyên lý kỹ thuật định vị dựa trên Wifi, đề xuất giải pháp nhằm nâng cao độ chính xác, tối ưu thời gian định vị của hệ thống định vị trong nhà sử dụng kỹ thuật định vị dựa trên dấu vân tay Wifi RSSI. Nghiên cứu của TS. Vũ

Trung Kiên đã giải quyết được hai vấn đề cơ bản liên quan đến định vị dựa trên Wifi: giải pháp nâng cao độ chính xác, tối ưu thời gian định vị của hệ thống định vị trong nhà sử dụng nguyên lý kỹ thuật Wifi RSSI. Đề tài luận án này chưa đề cấp đến các kỹ thuật định vị khác [4].

- Bộ Thông tin và Truyền thông có quy định khung tham chiếu về hệ thống định vị, trong đó có định vị di động dựa trên máy cầm tay, sử dụng số liệu định vị GPS của máy di động cầm tay, cho các ứng dụng đô thị như quản lý giao thông, địa chính v.v…Khung tham chiếu này chỉ đưa ra các khái niệm, quy định tiêu chuẩn liên quan đến kỹ thuật định vị dựa trên máy cầm tay (số liệu GPS máy cầm tay) cho các ứng dụng đô thị mà chưa đưa ra kỹ thuật cụ thể [5].

Hiện NCS chưa tìm thấy công trình khoa học nào trong nước được công bố liên quan đến định vị thiết bị di động 4G ứng dụng cho công tác an ninh.

1.4.1.2. Tài liệu tiếng Anh

Luận án đã tổng hợp và nghiên cứu một số vấn đề được công bố trong các bài báo khoa học, tiêu chuẩn kỹ thuật về định vị di động nói chung và định vị di động 4G/LTE liên quan đến đề tài luận án như sau:

- Sách kỹ thuật của tác giả Ayad M.H. Khaled, Ấn Độ, năm 2010, đã đưa ra những nghiên cứu tổng quan về phân loại các hệ thống định vị vô tuyến và ứng dụng của nó, các nguyên lý kỹ thuật và thuật toán tính toán xác định vị trí trong định vị vô tuyến nói chung, định vị điện thoại di động nói riêng. Tác giả khẳng định định vị vô tuyến là một tính năng cốt lõi của các mạng vô tuyến thế hệ tương lai, cho phép ứng dụng cho quân sự, an ninh công cộng và thương mại và cần phải có các nghiên cứu để nâng cao hiệu quả định vị đặc thù cho mỗi loại ứng dụng [23].

- Bài báo của tác giả Andreas Schmidth – Dannert, đại học kỹ thuật Berlin – Đức, vào năm 2012, nghiên cứu sự khác nhau về độ chính xác và chi phí giữa các kỹ thuật và cơ chế định vị thiết bị di động, trên cơ sở đó có các khuyến nghị sử dụng kỹ thuật định vị cho các ứng dụng khác nhau [24].

- Bộ luật về Thông tin vô tuyến và An ninh công cộng của Mỹ, năm 1999, đưa ra các dịch vụ, các tiêu chuẩn và yêu cầu kỹ thuật của FCC về dịch vụ 911 và E911 [25].

- Tác giả Brian O'Keefe, năm 2017, công bố nghiên cứu về kỹ thuật định vị ToA và TDoA. Trong đó, tác giả khẳng định việc tính toán chính xác vị trí của đối tượng mục tiêu là vấn đề cốt lõi, sống còn đối với các hệ thống định vị dẫn đường như Google Maps, khuyến nghị sử dụng các kỹ thuật ToA và TDoA cho các ứng dụng đó. Tác giả cũng nhấn mạnh, "nếu anh không biết anh ở đâu, anh sẽ không thể biết anh đang đi đâu" [26].

- Các tác giả M.F.M. Mahyuddin, A.A.M. Isa, M.S.I.M.Zin, Afifah Maheran A.H, Z.Manap and M.K.Ismail, Đại học Tổng hợp Malaysia, đã đưa ra các luận giải tổng quan về các kỹ thuật định vị cho công nghệ LTE, qua đó các tác giả khuyến nghị sử dụng kỹ thuật lai ghép cho định vị LTE và đề nghị tiếp tục nghiên cứu trong môi trường mạng LTE phát triển, thay đổi [32].

- Tác giả Rafael Saraiva Campos, năm 2017, đưa ra các nghiên cứu về lộ trình và phương pháp áp dụng để cải tiến các kỹ thuật định vị thiết bị di động khi mạng di động phát triển từ 2G, 3G đến 4G. Trong đó, tác giả đưa ra các khuyến nghị các vấn đề cần nghiên cứu để có thể cải tiến kỹ thuật định vị khi mạng phát triển lên 4G [33].

- Tập đoàn R&S (Đức), một trong những nhà sản xuất lớn nhất thế giới về thiết bị vô tuyến điện, một trong những thành viên của ITU-R giới thiệu công nghệ cho các dịch vụ LCS trong mạng LTE. Trong đó, khuyến nghị một số tiêu chuẩn cần áp dụng, phát triển cho dịch vụ này trên mạng LTE [35].

-Tập đoàn Erisson (Thụy Điển), một nhà sản xuất lớn trên thế giới, thành viên ITU về công nghệ điện thoại di động, trong sách trắng về định vị với LTE, đã có các khuyến nghị về các thuận lợi và khó khăn cần giải quyết khi triển khai định vị di động trong mạng LTE [36].

- Các tác giả Zhang Bo, Du Yuanfeng, and Yang Dongkai (Trung Quốc), năm 2015, công bố các nghiên cứu về các tính năng mới của kỹ thuật định vị trong các hệ thống LTE-A mà các hệ thống định vị ứng dụng [37].

- Các tác giả Pedro J. Fernández, José Santa, and Antonio F. Skarmeta, năm 2020, công bố nghiên cứu đề xuất và đánh giá về định vị lai ghép cho các không gian thông minh. Trong đó, các tác giả chỉ ra một số vấn đề cần thay đổi cho kỹ thuật định

vị lai ghép, như cần nghiên cứu ứng dụng các kỹ thuật và thuật toán mới để đảm bảo khả năng định vị hiệu quả trong các không gian thông minh [38].

- SPIRENT, 2018, Mỹ, công bố nghiên cứu tổng quan về định vị LTE. Trong đó, đưa ra các vấn đề cần nghiên cứu sâu hơn khi áp dụng kỹ thuật định vị cho mạng di động LTE [43].

- Các tác giả Jose A. del Peral-Rosado, Jose A. Lopez-Salcedo, Gonzalo Seco-Granados, Francesca Zanier, and Massimo Crisci, năm 2012, công bố các phân tích cơ bản về khả năng định vị trong 3GPP LTE [44].

- Các tác giả Juan Luis Bejarano-Luque, Matías Toril, Mariano Fernández-Navarro, Luis Roberto Jiménez and Salvador Luna-Ramírez, năm 2021, công bố về khả năng và các khó khăn khi định vị người dùng trên cơ sở các thông tin trên mạng xã hội. Các tác giả khuyến cáo cần nghiên cứu thu thập dữ liệu lớn để tổng hợp thông tin cả từ mạng di động LTE và cơ sở dữ liệu địa lý của mạng xã hội trong thời gian thực khi định vị người dùng [45].

- Một số tài liệu đưa ra các tiêu chuẩn kỹ thuật quốc tế liên quan đến tiêu chuẩn và trao đổi thông tin IMSI/IMEI, lỗ hổng bảo mật trong các mạng di động và một số phương pháp thu thập thông tin IMSI/IMEI qua giao diện vô tuyến. Một số tài liệu nghiên cứu chung về kỹ thuật thu chặn chủ động và bị động giao diện vô tuyến di động. Tuy nhiên, mạng di động nước ta có nhiều đặc thù riêng, trong khi đó các tài liệu chỉ đưa ra được các nguyên tắc, kỹ thuật chung, cần khảo sát nghiên cứu cụ thể môi trường mạng di động hỗn hợp của nước ta mới có giải pháp kỹ thuật khả thi [46-54].

- Một số tài liệu của các hãng công nghệ chuyên dùng cho an ninh nêu tính năng của các hệ thống kỹ thuật định vị địa lý trên cơ sở thu thập thông tin từ nhà mạng di động, thu thập thông tin qua đường báo hiệu viễn thông hoặc hệ thống định vị lai ghép trên cơ sở thu thập thông tin từ nhiều nguồn. Tuy nhiên, các tài liệu này chỉ giới thiệu tính năng chung và ứng dụng, không có giải pháp, nguyên lý kỹ thuật [46-58].

1.4.2. Những tồn tại, hạn chế và thách thức

1.4.2.1. Một số tồn tại về cơ sở khoa học, nguyên lý kỹ thuật

Qua khảo sát các công trình nghiên cứu khoa học trong và ngoài nước, tài liệu đăng tải trên mạng Internet, các tiêu chuẩn kỹ thuật quốc tế, sách trắng của các nhà cung cấp thiết bị viễn thông di động 4G-LTE và tổng hợp về các tài liệu điển hình ở trên, luận án nhận thấy có một số tồn tại như sau về cơ sở khoa học, nguyên lý kỹ thuật liên quan đến việc tìm kiếm, đề xuất giải pháp kỹ thuật hệ thống định vị:

- Chưa tìm thấy tài liệu nào công bố về công trình nghiên cứu tổng quát hoặc cụ thể giải pháp kỹ thuật định vị thiết bị di động 4G ứng dụng cho an ninh.

- Các nghiên cứu khoa học được nêu ở phần trên chỉ giải quyết các vấn đề kỹ thuật chung về định vị di động, trong đó có định vị di động 4G/LTE; một số nghiên cứu về một trong những phương pháp giải bài toán cụ thể về định vị 4G/LTE; một số tài liệu mô tả về các đạo luật của Mỹ liên quan đến định vị di động phục vụ cứu hộ khẩn cấp E911; một số tài liệu giới thiệu về khả năng cung cấp hệ thống định vị địa lý hoặc hệ thống định vị di động lai ghép (Hybrid Positioning System), trong đó mô tả nâng cao chất lượng (độ chính xác định vị) đối với định vị dựa trên dữ liệu môi trường mạng, Wifi. Tuy nhiên, chưa thấy những tài liệu, công trình nào công bố chính thức, đầy đủ về lĩnh vực nghiên cứu cần thiết của đề tài luận án.

- Các công trình khoa học ở trong và ngoài nước đã đặt vấn đề và đưa ra nhiều khuyến nghị cần nghiên cứu, giải quyết đối với định vị di động trong môi trường mạng 4G, các kỹ thuật định vị di động cần cải tiến, các vấn đề về thu thập dữ liệu lớn giữa dữ liệu mạng 4G-LTE và dữ liệu môi trường mạng xã hội để nâng cao hiệu quả định vị v.v…

1.4.2.2. Một số hạn chế và thách thức trong thực tế

Việc xây dựng hệ thống kỹ thuật định vị thiết bị di động thế hệ thứ tư ứng dụng cho công tác an ninh sẽ gặp các khó khăn, thách thức cơ bản như sau:

- *Về chính sách*: Chưa có đủ các chính sách để có thể thiết lập các hệ thống trung gian tại nhà mạng di động và nhà mạng Internet (theo tiêu chuẩn quốc tế của ITU) cũng như các kết nối để thu thập dữ liệu từ các đầu vào một cách đầy đủ, cần thiết.

- *Về kỹ thuật và thực tiễn:* Mạng di động và Internet Việt Nam phát triển, thay đổi nhanh chóng, liên tục, các mạng viễn thông được phân chia thành 3 khu vực (Bắc, Trung, Nam), mạng di động và Internet Việt Nam sử dụng hàng loạt công nghệ từ nhiều nhà cung cấp thiết bị khác nhau. Do vậy, sẽ có quá nhiều điểm mạng về vật lý cần kết nối, truy nhập để lấy dữ liệu định vị nhưng về nguồn lực sẽ không cho phép thực hiện mà chỉ có thể kết nối truy nhập vào một phần của mạng.

- *Về hoạt động của đối tượng:* Các đối tượng, mục tiêu cần định vị sử dụng đa dạng thiết bị đầu cuối di động, nhiều dịch vụ, nhiều mạng, nhiều thế hệ công nghệ. Ví dụ một đối tượng có thể liên lạc thoại/SMS thông thường qua 2G, liên lạc dữ liệu qua 3G/4G/Wifi một cách ngẫu nhiên hay có chủ đích; có thể thay đổi SIM điện thoại; có thể dùng nhiều SIM, nhiều mạng cùng lúc, có thể di động/di chuyển vùng địa lý.

- *Về nguồn lực*: Nguồn lực tài chính để xây dựng, trang bị những hệ thống, thiết bị kỹ thuật chuyên dụng cần thiết luôn hạn chế.

1.4.3. Hướng giải quyết

Luận án đề xuất hướng giải quyết những tồn tại, hạn chế và thách thức nêu trên bằng việc nghiên cứu các vấn đề cần thiết sau:

- Nghiên cứu các yêu cầu cụ thể, đặc thù của bài toán định vị di động.
- Nghiên cứu về các nguyên lý kỹ thuật định vị di động để tìm ra giải pháp có hiệu quả định vị thiết bị di động 4G trong điều kiện thực tế;
- Nghiên cứu đề xuất mô hình hệ thống kỹ thuật tổng thể để định vị thiết bị di động thế hệ thứ tư ứng dụng cho công tác an ninh.
- Nghiên cứu cách thức để phân loại, xác định một đối tượng để áp dụng đúng nguyên lý kỹ thuật, thuật toán định vị.
- Nghiên cứu giải pháp mở rộng cách thu thập dữ liệu từ nhiều nguồn khác nhau, tích lũy dữ liệu để nâng cao hiệu quả định vị; thực nghiệm thu thập dữ liệu Cell-ID từ nguồn mở.
- Nghiên cứu giải pháp kỹ thuật và thực nghiệm cải thiện độ chính xác của một số kỹ thuật định vị.

- Nghiên cứu cách thức bảo mật để chuyển giao, khai thác kết quả định vị cho các mục đích khác nhau.

- Nghiên cứu giải pháp kỹ thuật và thực nghiệm thu thập tham số IMSI/IMEI, hỗ trợ tìm kiếm, định vị đối tượng.

1.5. Kết luận Chương 1

Chương 1 đã nêu các luận giải tổng quan, cơ bản về các vấn đề nghiên cứu, trong đó đã xác định được mục tiêu cụ thể đặt ra của đề tài luận án; những định nghĩa, khái niệm, các thông tin, tầm quan trọng và ý nghĩa của vấn đề nghiên cứu mà đề tài luận án đặt ra; nghiên cứu tổng quan các nguyên lý kỹ thuật định vị; xác định các yêu cầu của định vị thiết bị di động đối với công tác an ninh.

Chương 1 cũng đã phân tích, luận giải về những giả thuyết, lý giải trước đây, các công trình nghiên cứu trong, ngoài nước về định vị di động, định vị di động 4G, định vị di động 4G phục vụ công tác an ninh; đã xác định được những tồn tại về vấn đề nghiên cứu, các hạn chế, thách thức về kỹ thuật và thực tế mà đề tài phải giải quyết, hướng giải quyết các vấn đề đó.

Trên cơ sở đó, Chương 1 xác định được các nội dung nghiên cứu cụ thể cần thực hiện để đáp ứng mục đích của đề tài luận án. Các kết quả nghiên cứu của Chương 1 là cơ sở cho đề xuất giải pháp kỹ thuật ở Chương 2; đề xuất mô hình hệ thống kỹ thuật và ứng dụng cho công tác an ninh ở Chương 3; thực nghiệm minh chứng giải pháp, mô hình hệ thống ở Chương 4.

CHƯƠNG 2. GIẢI PHÁP KỸ THUẬT NÂNG CAO HIỆU QUẢ ĐỊNH VỊ THIẾT BỊ DI ĐỘNG

Kết quả nghiên cứu ở Chương 1 đã chỉ ra rằng: Không có nguyên lý kỹ thuật định vị di động cơ bản nào là hiệu quả, khả thi, khả dụng cho mọi trường hợp; Yêu cầu định vị thiết bị di động thế hệ thứ tư ứng dụng cho công tác an ninh rất đa dạng và có nhiều đặc thù; Còn có nhiều tồn tại về cơ sở khoa học và nguyên lý kỹ thuật cũng như hạn chế, thách thức trong thực tế đối với bài toán định vị thiết bị di động thế hệ thứ tư ứng dụng cho công tác an ninh cần nghiên cứu, giải quyết.

Do vậy, yêu cầu cấp thiết đặt ra là cần phải có một giải pháp kỹ thuật định vị mới có hiệu quả. Trên cơ sở đó, nội dung Chương 2 sau đây xác định các yêu cầu cụ thể của bài toán định vị và đề xuất giải pháp kỹ thuật giải quyết những yêu cầu đó.

2.1. Xác định các yêu cầu cụ thể của bài toán định vị

2.1.1. Mô tả yêu cầu

- **Yêu cầu chung**

- Xác định đối tượng, mục tiêu định vị.
- Thu thập dữ liệu, xử lý, xác định vị trí của đối tượng, mục tiêu (Vị trí của đối tượng, mục tiêu được quy đồng là vị trí của thiết bị di động).
- Xác định được đối tượng trong phạm vi rộng, phạm vi tương đối, phạm vi hẹp và đến vị trí chính xác.
- Truy vết đối tượng.

- **Dữ liệu đầu vào**

- Dữ liệu từ mạng di động;
- Dữ liệu từ máy cầm tay;
- Dữ liệu từ SIM;
- Dữ liệu từ Wifi;
- Dữ liệu môi trường mạng mở.
- Kết hợp các loại dữ liệu.

- **Dữ liệu tham chiếu**

- Dữ liệu thuê bao di động;
- Dữ liệu địa lý.
- Và các dữ liệu khác liên quan.

- **Bài toán kỹ thuật**

- Xây dựng cơ sở dữ liệu định vị di động.
- Định vị đối tượng di động bằng các thuật toán dựa trên một trong hoặc nhiều dữ liệu đầu vào như các kỹ thuật định vị di động đã phân tích bằng các thuật toán khác nhau, tùy theo tính khả dụng của đầu vào và yêu cầu, tương ứng với kết quả đầu ra khác nhau.
- Tính toán kết hợp với các dữ liệu tham chiếu để đưa ra kết quả.

- **Đầu ra**

- Số liệu vị trí phạm vi rộng và thể hiện trên bảng thông tin;
- Số liệu vị trí phạm vi tương đối và thể hiện trên bảng thông tin;
- Số liệu vị trí phạm vi hẹp và thể hiện trên bản đồ số cùng trường thông tin;
- Tọa độ địa lý và thể hiện trên bản đồ số cùng trường thông tin;
- Đường đi của đối tượng, thể hiện trên bản đồ số;
- Mối quan hệ của đối tượng, thể hiện trên đồ thị quan hệ.

2.1.2. Khái niệm mới về đối tượng của bài toán định vị

Mỗi đối tượng, mục tiêu định vị đều có thể sử dụng nhiều thiết bị di động 4G hoạt động trong nhiều môi trường mạng khác nhau. Do đó, đối tượng của bài toán định vị được qui về một thiết bị di động 4G, nó có thể là máy điện thoại di động, máy tính bảng, máy tính xách tay,… có gắn modul kết nối 4G/LTE/Wifi/Bluetooth. Các thiết bị đó hoạt động trên môi trường mạng 4G và chủ yếu được sử dụng để liên lạc (như gọi điện thoại, nhắn tin, kết nối truy cập Internet, giao tiếp mạng xã hội…) hay các hành động khác (như chụp ảnh, ghi âm, quay phim và truyền về nơi khác …). Đối tượng có thể sử dụng liên lạc bằng các dịch vụ gọi điện, nhắn tin truyền thống hoặc bằng các dịch vụ trên nền Internet. Do vậy, nếu thông qua theo dõi hoạt động của thiết bị di động 4G mà đối tượng mang theo, có thể xác định được thông tin về đối tượng (danh tính, vị trí hiện tại, vị trí sắp đến, liên hệ/quan hệ với ai,.. Trong đó, việc

định vị, truy vết được đối tượng đó là quan trọng và thường xuyên nhất. Việc truy vết được đối tượng cũng sẽ xác định được các thông tin về đối tượng.

Nếu đã biết được đối tượng đó đăng ký và đang sử dụng một thuê bao di động 4G, thì có thể tìm được đối tượng thông qua việc định vị thuê bao đó. Cũng có thể thực hiện một cách dễ dàng hơn là hỏi nhà mạng di động thuê bao đó đang ở đâu (như trường hợp dịch vụ cứu hộ E911). Nhưng nếu không biết được đối tượng đang sử dụng thuê bao nào hoặc đối tượng sử dụng thiết bị di động 4G nhưng không phát sinh một cuộc gọi di động nào mà chỉ dùng để truy cập Internet, mạng xã hội hay đơn giản là liên lạc qua mạng thì bài toán định vị trở lên hết sức khó khăn. Khó khăn đầu tiên chính là làm thế nào để xác định được đối tượng đó. Do vậy, bài toán định vị đối tượng không còn thông thường là triển khai định vị ngay một thiết bị hay một số thuê bao di động 4G hoặc một thiết bị di động 4G nào đó mà trước tiên phải xác định được đối tượng, sau đó mới có được các dữ kiện chính xác cho bài toán định vị phù hợp sẽ áp dụng. Một đối tượng có thể được xác định chính xác bằng một tập các đặc điểm của nó. Qua thời gian, còn có các thông tin khác có thể xuất hiện như đối tượng đang ở đâu, làm việc gì, đi xe gì, xe của đối tượng đã xuất hiện những chỗ nào, đang truy cập Internet, mạng xã hội ở đâu.

(Lưu ý rằng ban đầu, việc xác định ở đâu là tương đối, ví như đang ở nước nào/ thành phố nào/ khu vực nào bằng cách thông qua xác định địa chỉ IP mà đối tượng đang online trên Internet, mạng xã hội).

Về mặt kỹ thuật và dịch vụ di động, một con người thường được gắn với một số thuê bao di động nào đó (và ngược lại, từ một số thuê bao di động có thể truy vấn dữ liệu thuê bao của nhà mạng ra một con người nào đó đăng ký thuê bao). Khi thuê bao phát sinh một cuộc gọi, dữ liệu liên quan đến cuộc gọi đó (CDR) có nhiều thông tin như: mã nước, mã mạng di động, mã vùng di động, Cell-ID và Cell-LAC di động phục vụ, số bị gọi v.v…Từ các thông tin này, nếu trong trường hợp thuê bao gọi trên nền mạng 2G, có thể xác định được thuê bao tức đối tượng đó ở đâu (một cách tương đối) và đang liên hệ với ai (tức mối liên hệ của đối tượng đó). Nhưng nếu số thuê bao đó xuất hiện cuộc gọi nhưng đó là cuộc gọi trên nền mạng 3G/4G hay đơn thuần chỉ

truy cập Internet/ Facebook…, mà User Name của dịch vụ đó lại được đăng ký từ một số thuê bao di động khác đồng thời lại ẩn danh thì việc xác định đó có là đối tượng cần truy tìm hay không là bài toán nan giải. Từ đây, việc định vị một đối tượng không thể chỉ thực hiện bằng cách định vị một số thuê bao di động nào đó mà đối tượng sử dụng như các nguyên lý định vị thông thường. Muốn định vị được một đối tượng hoạt động trên nền mạng 4G với đa dạng dịch vụ, đa dạng thiết bị như nói ở trên, trước tiên phải tìm kiếm một loạt thông tin khác nhau, từ đó xác định ra thông tin chính xác về đối tượng rồi mới có dữ kiện đưa vào bài toán định vị.

Gần đây, các nước tiên tiến đã mở rộng, đổi mới khái niệm về đối tượng, mục tiêu khi tiến hành định vị. Khái niệm này khá trừu tượng, cũng gần giống như nguyên lý triết học mà một con người bao giờ cũng nằm trong mối quan hệ tổng hòa của xã hội. Có thể nói tóm tắt, khái niệm về đối tượng đã được đổi mới, mở rộng sang khái niệm về mối liên hệ của nó, đối tượng không chỉ là ai như khi xác định đối tượng là một con người (hay số thuê bao di động của nó) mà chính là một tập đặc trưng của câu hỏi trên: ai, ở đâu, đi đâu, quan hệ với ai, làm gì, làm thế nào và mở rộng hơn là đi xe gì, sở thích gì, khám bệnh gì, hay đến đâu, mục đích và xu hướng của nó.

Đồng thời, với sự phát triển của công nghệ và dịch vụ số, mỗi đối tượng có hàng loạt thông tin xã hội liên quan có sẵn. Các thông tin liên quan đến nhau sẽ cùng xuất hiện và phải xác minh khi thực hiện một giao dịch trực tuyến nào đó. Tương tự đó, với mỗi đối tượng cần định vị, mà lại sử dụng thiết bị di động hoạt động trong môi trường mạng 4G thì việc xác định đối tượng đó không chỉ là dựa trên một dữ kiện mà phải là hàng loạt, hay một tập dữ kiện đặc trưng của nó và các dữ kiện liên quan đến nó. Tập dữ kiện đó được định nghĩa bằng một khái niệm mới mang các đặc trưng của đối tượng nằm trong mối liên hệ của nó và được gọi là một "**Thực thể**", trong tiếng Anh là "**Entity**".

Chẳng hạn, khi cần tìm kiếm một đối tượng, họ không chỉ định vị một đối tượng hay một số thuê bao di động cụ thể mà họ sẽ phân tích một loạt các dữ liệu, sự kiện liên quan của nó, tức phân tích, tìm kiếm một "thực thể". Các dữ kiện "thực thể" đó có thể được phân tích từ các nguồn khác nhau có thể có như dữ liệu điện thoại di động/điện

thoại vệ tinh/vị trí IP/facebook/GPS được trích xuất từ hình ảnh..., và loại của nó (IMSI/MSISDN/IMEI/TMSI/IP,...). Ngoài ra, cũng cần truy vấn, phân tích bổ sung trên các cơ sở dữ liệu tham chiếu, đã được làm giàu và từ đó sẽ tự động cảnh báo được các chỉ dẫn, hành vi đáng ngờ, hay đơn giản là xu hướng của nó.

2.1.3. Mô tả yêu cầu kỹ thuật cụ thể

Yêu cầu kỹ thuật cụ thể của bài toán định vị thiết bị di động thế hệ thứ tư được mô tả chi tiết trong bảng 2.1.

Bảng 2. 1. Yêu cầu kỹ thuật cụ thể của bài toán định vị

TT	Mô tả	Yêu cầu kỹ thuật, tham số, trị số
1	**Yêu cầu chung**	
1.1	**Xác định đối tượng định vị**	
	Loại đối tượng	"Thực thể"
	Mô tả thực thể	Tập dữ liệu đặc trưng và dữ liệu liên quan đến đối tượng
	Tên người	Có
	Số thuê bao điện thoại MSISDN	Có
	Địa chỉ địa lý	Có
	Địa chỉ IP sở hữu hoặc sử dụng	Có
	Thuê bao (account) Internet	Có
	Nick Name mạng xã hội	Có
	Các thông tin xã hội khác	Có
1.2	**Định vị đối tượng**	Các trị số yêu cầu (tính khả dụng, độ chính xác… tương ứng với các số liệu nguyên lý kỹ thuật đã phân tích, so sánh ở Chương 1.
	Đối tượng của bài toán	Thiết bị di động mà đối tượng mang theo
	Loại thiết bị di động	Điện thoại di động, máy tính bảng, máy tính xách tay, modul di động
	Định vị phạm vi rộng của đối tượng	Quốc gia, vùng lãnh thổ
	Định vị phạm vi tương đối của đối tượng	Tỉnh, thành phố
	Định vị phạm vi hẹp của đối tượng	Ô di động (Cell-ID/ Cell LAC), Sector BTS/eNB
	Định vị vị trí chính xác của đối tượng	Tọa độ địa lý, số nhà, đường phố, tòa nhà, căn phòng…
	Truy vết đối tượng	Lịch sử vị trí, đường đi
	Xác định mối quan hệ của đối tượng	Mối quan hệ liên lạc, biểu đồ quan hệ

TT	Mô tả	Yêu cầu kỹ thuật, tham số, trị số
2	**Thu thập dữ liệu đầu vào của bài toán định vị**	
	Dữ liệu từ mạng di động và mạng báo hiệu	- Cell-ID, Cell LAC phục vụ, số gọi, số bị gọi, thời gian cuộc gọi, loại cuộc gọi …được lập thành cơ sở dữ liệu chi tiết cuộc gọi (CDR). - Dữ liệu của mạng di động: MCC, MNC, Cell-ID database - Dữ liệu của mạng báo hiệu: SPC…
	Dữ liệu từ máy cầm tay	IMSI, IMEI và các tham số vô tuyến, tham số GNSS
	Dữ liệu từ SIM	MSISDN và các tham số định danh
	Dữ liệu từ Wifi	Các tham số của Wifi Access Point và các tham số vô tuyến
	Dữ liệu môi trường mạng mở	-Tất cả dữ liệu liên quan đến truy cập Internet, sử dụng mạng xã hội, sử dụng dịch vụ OTT như IP Address, Iternet Account, FB Acount, Nick Name, Media…. - Dữ liệu Cell-ID toàn cầu từ nguồn mở - Dữ liệu Wifi toàn cầu từ nguồn mở
3	**Thu thập dữ liệu tham chiếu của bài toán định vị**	
	Dữ liệu thuê bao di động	Cơ sở dữ liệu thuê bao của nhà mạng
	Dữ liệu địa lý	Bản đồ số, bản đồ hành chính, bản đồ Google Maps.
	Dữ liệu khác liên quan	Những dữ liệu liên quan đến hoạt động xã hội khác như mô tả ở khái niệm đối tượng
4	**Đầu ra của bài toán định vị**	
	Số liệu vị trí phạm vi rộng	Có, theo phạm vị quốc gia, vùng lãnh thổ
	Số liệu vị trí phạm vi tương đối	Có, theo phạm vi tỉnh, thành phố
	Số liệu vị trí phạm vi hẹp	Có, theo bán kính Cell di động
	Số liệu vị trí chính xác	Có
	Truy vết lịch sử vị trí và đường đi	Có, theo độ chính xác của bản đồ số Google Map (trực tuyến hoặc không trực tuyến) hoặc theo độ chính xác của bản đồ số chuyên dụng (nếu cài đặt và sử dụng)
	Xác định đồ thị mối quan hệ	Có, đồ thị GraphTech mối quan hệ.

Một số dữ liệu đầu vào và dữ liệu tham chiếu cụ thể sẽ được mô tả chi tiết ở Bảng 2.2

2.2. Đề xuất giải pháp kỹ thuật tổng thể

Căn cứ vào các kết luận rút ra nêu trên, luận án đề xuất giải pháp kỹ thuật định vị thiết bị di động thế hệ thứ tư như sau:

2.2.1. Lựa chọn nguyên lý kỹ thuật định vị lõi

Do không có nguyên lý kỹ thuật nào là hiệu quả, khả dụng trong mọi trường hợp, trong khi đó, yêu cầu của bài toán định vị thiết bị di động thế hệ thứ tư rất đa dạng, đặc thù, sau khi nghiên cứu tham khảo các tài liệu [32-45] và kết quả phân tích ở phần mở đầu và Chương 1, luận án đề xuất sử dụng nguyên lý kỹ thuật lõi **"Hệ thống định vị lai ghép"** để định vị thiết bị di động thế hệ thứ tư.

2.2.1.1. Mô tả nguyên lý kỹ thuật "Hệ thống định vị lai ghép"

Hệ thống định vị lai ghép sử dụng kết hợp các công nghệ dựa trên mạng và dựa trên thiết bị cầm tay để xác định vị trí. Một ví dụ điển hình là phương pháp sử dụng một số chế độ của GPS có Hỗ trợ (A-GPS), có thể sử dụng cả dữ liệu GPS và thông tin mạng để tính toán vị trí của thiết bị cầm tay. Cả hai loại dữ liệu này đều được thiết bị di động sử dụng để làm cho vị trí của nó chính xác hơn (tức là kỹ thuật A-GPS). Kỹ thuật định vị lai ghép cũng có thể thực hiện bằng cách để thiết bị di động thu được vị trí GPS của nó trực tiếp từ vệ tinh, sau đó gửi thông tin qua mạng tới người đang muốn xác định vị trí của thiết bị di động. Các hệ thống sử dụng kỹ thuật định vị lai ghép điển hình bao gồm: dịch vụ định vị của Google Maps, dịch vụ OTDoA và E-CellID của mạng 4G-LTE.

Ngoài ra, hệ thống định vị lai ghép còn có một cách tiếp cận vị trí khác. Hệ thống sẽ kết hợp một số phương pháp xác định vị trí khác nhau để định vị thiết bị di động bằng Wi-Fi, WiMAX, GSM, 4G-LTE, địa chỉ IP và dữ liệu môi trường mạng thiết bị di động truy cập, liên lạc.

2.2.1.2. Khái quát "Hệ thống định vị lai ghép tiên tiến"

Với mục tiêu định vị thiết bị di động thế hệ thứ tư, yêu cầu là định vị không chỉ thiết bị điện thoại di động (điện thoại di động ở các thế hệ 2 hoặc 3 hoặc 4G hoặc điện thoại 4G hỗ trợ hoạt động ở cả 2, 3G; có thể hoạt động chỉ ở 1 chế độ hoặc cùng lúc hoạt động được ở cả 3 chế độ, tùy thuộc độ khả dụng của mạng hoặc thiết lập của người dùng) mà còn cần định vị cả các thiết bị di động/cơ động sử dụng kết nối điện thoại 4G và/hoặc Wifi (như máy tính bảng, máy tính xách tay, các loại thiết bị thông tin liên lạc khác có sim 4G và/hoặc bảng mạch kết nối Wifi).

Bên cạnh đó, cũng cần định vị cả các thiết bị di động đa mạng như thiết bị điện thoại vệ tinh có hỗ trợ sẵn SIM điện thoại di động 4G mặt đất hoặc bộ tương thích điện thoại di động vệ tinh với mạng di động mặt đất (3 loại điện thoại di động vệ tinh chủ yếu trên thế giới là Inmasat iSatphone Pro, Iridium và Thuraya đều có khả năng tương thích, hoạt động song song cả với mạng di động mặt đất 3G/4G, đã cung cấp dịch vụ).

Do vậy, sau khi nghiên cứu, luận án đề xuất giải pháp kỹ thuật **"Hệ thống định vị lai ghép tiên tiến"** bằng cách tiếp cận vị trí từ không chỉ lai ghép hai kỹ thuật định vị dựa trên mạng và định vị dựa trên máy cầm tay với các mạng GSM, 4G-LTE mà còn sử dụng cả định vị dựa trên SIM, trên Wifi, Wimax, trong đó thu thập và phân tích cả các dữ liệu địa chỉ IP Address và dữ liệu môi trường mạng mà nó truy cập, liên lạc.

"Hệ thống định vị lai ghép tiên tiến" sẽ thu thập, xử lý kết hợp đa đầu vào dữ liệu để nâng cao hiệu quả định vị, đồng thời xử lý cả các dữ liệu tham chiếu nếu cần thiết để cho ra đa dạng các kết quả đầu ra tùy theo mục đích, yêu cầu.

Hệ thống này cũng sẽ có khả năng phát triển, mở rộng lâu dài, ví dụ định vị thiết bị di động thế hệ thứ 5 (5G) bởi được xây dựng trên một nền tảng mở cả về nguyên lý kỹ thuật, phần mềm và phần cứng, cho phép thêm đầu vào, tăng dung lượng, tốc độ xử lý, cung cấp, cải tiến, mở rộng các giao diện lập trình ứng dụng (API), bổ sung, cải tiến các thuật toán định vị để có các kết quả đầu ra khác nhau theo yêu cầu.

2.2.2. Giải pháp kỹ thuật kết hợp đa dạng nguồn dữ liệu để nâng cao hiệu quả định vị

2.2.2.1. Yêu cầu

Như đã phân tích ở các phần trên, có nhiều phương pháp định vị di động. Mỗi phương pháp dựa trên các cơ sở khác nhau, sử dụng các công nghệ, kỹ thuật định vị khác nhau, mỗi kỹ thuật có các thuật toán định vị khác nhau và có các tiêu chí độ chính xác, độ tin cậy, độ khả dụng và khả năng ứng dụng khác nhau, trong những môi trường khác nhau và yêu cầu ứng dụng định vị cụ thể khác nhau. Như vậy, mỗi một loại ứng dụng định vị di động có thể sử dụng công nghệ, kỹ thuật định vị khác nhau hoặc sử dụng cùng lúc (lai ghép/hỗn hợp) nhiều công nghệ, kỹ thuật định vị khác nhau và sẽ sử dụng một hoặc nhiều loại dữ liệu đầu vào, dữ liệu tham chiếu khác nhau để thực hiện bài toán. Mục tiêu của đề tài luận án là nghiên cứu, tìm kiếm giải pháp kỹ thuật có hiệu quả định vị thiết bị di động 4G. Câu hỏi đặt ra là giải pháp kỹ thuật đó sẽ cần áp dụng các bài toán, nguyên lý kỹ thuật định vị gì, tức là sẽ cần những dữ liệu đầu vào, dữ liệu tham chiếu gì để xử lý. Rõ ràng là, để định vị một đối tượng, trước hết ta phải xác định được chúng, trên cơ sở phân loại chúng bằng các bài toán như bài toán phân lớp đã nêu ở trên, sau đó phải xác định rõ yêu cầu định vị và công nghệ khả dụng để thực hiện bài toán định vị. Các công nghệ định vị khác nhau, yêu cầu kết quả định vị khác nhau sẽ cần dữ liệu đầu vào và/hoặc dữ liệu tham chiếu khác nhau. Do vậy, để giải quyết được bài toán trên, căn cứ vào kết quả phân tích, nghiên cứu, so sánh các kỹ thuật định vị nêu trên, trước mắt cần đặt vấn đề nghiên cứu tìm hiểu bài toán xây dựng cơ sở dữ liệu định vị di động.

2.2.2.2. Lựa chọn giải pháp

Trong khái niệm đã được đề cập ở trên, một đối tượng hoạt động trên di động cũng đồng nhất với một thuê bao hay một thiết bị di động mà đối tượng đó sử dụng hay hay sở hữu, hoạt động hay không hoạt động. Nói một cách dễ hiểu hơn, một đối tượng có thể đang cầm giữ, sở hữu, sử dụng (có hoạt động kích hoạt cuộc gọi, kết nối hay không) một hay nhiều thiết bị di động như điện thoại di động, máy tính bảng,

máy tính xách tay (có bảng mạch kết nối Wifi hoặc sử dụng bảng mạch/USB 4G) và hiện đang ở đâu đó.

Nhiệm vụ quan trọng nhất là phải tìm ra đối tượng đó ở đâu, đi đâu, đã, đang và sẽ làm gì, đã, đang và sẽ liên hệ với ai. Bài toán ở đây chính là phải tìm ra thiết bị di động hoặc thuê bao di động mà đối tượng đó đang cầm nắm, sở hữu hoặc sử dụng. Bên cạnh đó, cũng phải chứng minh được điều ngược lại là chính đối tượng đó sử dụng thiết bị di động này. Trong một khía cạnh đơn giản nhất, tức là nếu phát hiện, tìm kiếm được một thiết bị di động nghi ngờ thì ai là người sở hữu, sử dụng hay ai là chủ thuê bao, ai là người đang hoạt động trên thiết bị đó.

Qua các phân tích cơ bản này, chúng ta nhận thấy rằng, để tìm kiếm chính xác được một đối tượng sử dụng thiết bị di động như bài toán/ câu hỏi đặt ra trên, chúng ta sẽ cần phải ứng dụng một loạt phương pháp định vị di động. Một loạt phương pháp kỹ thuật này sẽ phải xử lý hàng loạt dữ liệu đầu vào của bài toán định vị đồng thời phải xử lý cả các dữ liệu liên quan (tham chiếu) như: dữ liệu thuê bao điện thoại; dữ liệu địa lý (ở đâu, tọa độ nào, chỗ nào, địa chỉ nào, khu vực nào); dữ liệu đa phương tiện truy cập, kết nối mạng di động và Internet (cuộc gọi, cuộc truy cập, hình ảnh, âm thanh, các hoạt động trên mạng xã hội v.v…). Về mặt toán học, các dữ liệu đầu vào hoặc tham chiếu để xử lý như nêu trên càng nhiều, càng đa dạng thì phương pháp định vị càng khả dụng, cho được độ chính xác vị trí càng cao và kết quả trả ra càng nhanh chóng. Đồng thời, dữ liệu đầu vào và tham chiếu càng nhiều thì bài toán so sánh, nhận dạng chính xác đối tượng càng chính xác.

Tóm lại, dữ liệu đầu vào, tham chiếu và dữ liệu đầu ra của bài toán định vị di động thiết bị di động 4G đòi hỏi nhiều loại, đa dạng, có cấu trúc hoặc không có cấu trúc, càng lớn càng tốt và ngày càng lớn. Do vậy, với mục tiêu yêu cầu đã đặt ra, căn cứ vào tính chất của kỹ thuật định vị di động, luận án lựa chọn giải pháp xây dựng cơ sở dữ liệu định vị di động bằng cách sử dụng một "**Nền tảng dữ liệu mở**" để có thể thu thập, xử lý kết hợp đa dạng nguồn dữ liệu.

Các lý do chính để lựa chọn giải pháp nền tảng cơ sở dữ liệu mở cho định vị di động gồm:

- Cần xử lý nhiều loại dữ liệu, cả có cấu trúc (ví dụ như dữ liệu Cell-ID di động, dữ liệu chi tiết cuộc gọi di động CDR v.v…) và phi cấu trúc (như dữ liệu đa phương tiện trên mạng phát sinh từ thiết bị di động, dữ liệu bản đồ, địa lý v.v…).

- Cần xử lý nhiều đầu vào dữ liệu từ các nguồn cơ sở cho các loại kỹ thuật định vị khác nhau (dữ liệu mạng di động/mạng Internet mà thiết bị di động truy cập; dữ liệu từ máy cầm tay di động, dữ liệu SIM, dữ liệu Wifi, dữ liệu đa phương tiện v.v…), bao gồm cả loại dữ liệu thô và dữ liệu đã được lọc, phân loại.

- Cần xử lý dữ liệu cả trực tuyến và không trực tuyến.

- Cần lưu trữ, xử lý khối lượng dữ liệu ngày càng lớn đối với cả dữ liệu đầu vào và đầu ra đồng thời đòi hỏi tốc độ xử lý nhanh nên cần có các công nghệ mới để lọc, nén, phân loại dữ liệu và xử lý dữ liệu;

- Cần áp dụng công nghệ mới như học máy (ML) và trí tuệ nhân tạo (AI) cho việc thu thập, xử lý dữ liệu đầu vào cũng như hỗ trợ phân tích dữ liệu đầu ra.

- Phù hợp với xu thế của thế giới, các cơ sở dữ liệu lớn hiện và sẽ có như dữ liệu của Google, dữ liệu mạng di động 4G, 5G, các dữ liệu Cell-ID, Wifi nguồn mở cộng đồng.

- Yêu cầu bảo mật, đảm bảo an ninh, an toàn.

Trong bảng 2.2, luận án tiến hành thống kê, phân loại các loại dữ liệu đầu vào và/hoặc dữ liệu tham chiếu cho một nguyên lý kỹ thuật định vị hoặc yêu cầu kết quả (ứng dụng) định vị nào đó, đặc thù cho công tác an ninh; nguồn của nó và cách tiếp cận, thu thập [3-6], [32-45].

Bảng 2. 2. Các nguồn dữ liệu định vị

TT	Mô tả	Nguồn	Kỹ thuật thu thập	Mục đích chính/ Yêu cầu kết quả
I.	**Cơ sở dữ liệu BTS/eNB (**Cell-ID, Cell LAC, vị trí cột phát sóng)			
1		Từ mạng di động	- Kết nối vào mạng di động và lấy dữ liệu trực tuyến	- Lập cơ sở dữ liệu định vị; - Lập bản đồ Cell;

TT	Mô tả	Nguồn	Kỹ thuật thu thập	Mục đích chính/ Yêu cầu kết quả
			- Nhà mạng di động cung cấp qua tập dữ liệu BTS/eNB.	- Đầu vào cho một số thuật toán định vị.
2		Từ nguồn mở: -Open Cell-ID -Google	Giao diện lập trình ứng dụng (API) lấy số liệu BTS/eNB từ nguồn mở và Google.	
3		Từ nguồn cộng đồng	Giao diện lập trình ứng dụng (API)lấy cùng dữ liệu vị trí Wifi (đa số trong đó có Cell-ID).	
4		Từ mạng báo hiệu SS7	Truy vấn, tương tác với điểm báo hiệu quốc gia và điểm báo hiệu của mạng	Xác định vị trí tương đối (vùng Cell phục vụ); truy vết đường đi của thiết bị di động.
II	**Cơ sở dữ liệu vị trí Wifi**	Từ nguồn cộng đồng (crowd-sourced data), đa số trong đó có Cell-ID	Giao diện lập trình ứng dụng (API) lấy số liệu từ nguồn cộng đồng nào khả dụng; cho phép MAP.	- Lập cơ sở dữ liệu vị trí Wifi, cơ sở dữ liệu Cell-ID; - Định vị Wifi (thiết bị trong nhà).
1		Combain Positioning Service		
2		LocationAPI.org by Unwired Labs		
3		Mozila Location Services		
4		Mylnikov GEO		
5		Navizone		
6		radiocell.org		

TT	Mô tả	Nguồn	Kỹ thuật thu thập	Mục đích chính/ Yêu cầu kết quả
7		OpenWLANMap /openwifi.su		
8		WiGLE		
		(Các nguồn dữ liệu Wifi mở được mô tả chi tiết trong phụ lục)		
III	**Dữ liệu thuê bao** (Subscriber), **dữ liệu cuộc gọi** (CDRs list), **trạng thái hoạt động**			Xác minh đối tượng; xác minh liên lạc, vị trí tương đối (Cell), trạng thái hoạt động, lập đồ thị mối liên hệ của đối tượng.
1		Nhà mạng di động	Kết nối trực tuyến trao đổi dữ liệu (cho phép) hoặc cung cấp dữ liệu thuê bao và dữ liệu cuộc gọi offline theo yêu cầu.	
2		Mạng báo hiệu SS7	API thu thập dữ liệu cuộc gọi, trạng thái hoạt động	
IV	**Dữ liệu IMSI, IMEI, TMSI** (của thuê bao, máy di động)			
1		Nhà mạng di động	Nhà mạng cung cấp dữ liệu.	Định vị tầm xa (vùng Cell)
2		Mạng báo hiệu SS7	API thu thập dữ liệu IMSI, IMEI.	Định vị tầm xa (vùng Cell)
3		Kênh báo hiệu trên đường vô tuyến BTS/eNB-MS/UE	Thiết bị trạm gốc giả lập, phát hiện tham số IMSI, IMEI.	Xác minh sự có mặt của thuê bao; truy vết đường đi hoặc định vị tiếp cận.

TT	Mô tả	Nguồn	Kỹ thuật thu thập	Mục đích chính/ Yêu cầu kết quả
V	**Các tham số sóng vô tuyến**			
1		Từ BSC mạng di động	Trao đổi dữ liệu trực tuyến bởi truy cập vào BSC mạng di động.	Định vị tầm gần.
2		Từ trạm BTS/eNB	Thu tín hiệu vô tuyến bằng thiết bị định hướng cơ động tầm gần (thụ động, chủ động hoặc bán chủ động).	Định vị tầm gần, tiếp cận.
3		Từ MS/UE	Thu, giả lập BTS/eNB, tìm kiếm (homing) bằng thiết bị cơ động hoặc cầm tay.	Định vị tầm gần, tiếp cận.
VI	**Dữ liệu tọa độ MS/UE**	Từ mạng di động	API lấy dữ liệu GPS của MS từ mạng di động.	Định vị chính xác MS/UE, truy vết đường đi MS/UE và hiển thị trên bản đồ.
VII	**Dữ liệu vị trí MS/UE có sẵn**	Từ mạng di động hoặc các dịch vụ dựa trên vị trí LBS	API lấy dữ liệu từ mạng di động và các dịch vụ giá trị gia tăng dựa trên vị trí (ví dụ dịch vụ dẫn đường).	Xác minh đối tượng, định vị, truy vết MS/UE.
VIII	**Dữ liệu địa chỉ IP Address, dữ liệu Media mạng**	Từ mạng Internet/ mạng xã hội	API lấy dữ liệu mạng phục vụ tại khu vực MS truy cập.	Định vị tầm xa, so sánh, xác minh đối tượng.
IX	**Dữ liệu tham chiếu**			
1	Dữ liệu bản đồ địa lý, bản đồ hành chính	Goole Maps Online hoặc các cơ sở dữ liệu bản đồ Offline	API bản đồ.	Hiển thị, truy vết đường đi.

2.2.3. Giải pháp kỹ thuật cải thiện độ chính xác định vị

2.2.3.1. Yêu cầu về cải thiện độ chính xác định vị

Như kết quả nghiên cứu ở trên, luận án lựa chọn giải pháp kỹ thuật **"Hệ thống định vị lai ghép tiên tiến"**, tức là cải tiến hệ thống kỹ thuật định vị lai ghép trên cơ sở thu thập, xử lý đa dạng các nguồn thông tin nâng cao hiệu quả định vị thiết bị di động. Trong một hệ thống định vị lai ghép, căn cứ vào dữ liệu đầu vào có được, hệ thống sẽ áp dụng một trong các nguyên lý kỹ thuật để tính toán, đưa ra vị trí của thiết bị di động. Những nguyên lý kỹ thuật đó đã được nghiên cứu cơ bản, chuẩn hóa và có những thuật toán được công bố để có thể lập trình ứng dụng, thiết lập các API để xử lý và đưa ra kết quả định vị. Tuy nhiên, có nhiều nguyên nhân khác nhau dẫn đến khó tính toán được vị trí trên hệ tọa độ địa lý (với không gian 3 chiều) hoặc đưa ra kết quả không chính xác. Bên cạnh đó, trong thực tế, do sai số của các phép đo nên bài toán định vị có thể tính toán ra nhiều kết quả vị trí của thiết bị di động. Do vậy, bên cạnh việc cải tiến kỹ thuật định vị lai ghép nói chung, luận án đã nghiên cứu cải tiến, mở rộng một số thuật toán định vị có sẵn để có thể lập trình được các API tính toán vị trí ngày càng chính xác hơn. Một số nghiên cứu này đã có kết quả khả quan, trong đó có nghiên cứu cải tiến, mở rộng thuật toán cho kỹ thuật định vị ToA và AoA để xác định chính xác vị trí của một thiết bị di động hoạt động trong môi trường 4G/LTE.

2.2.3.2. Cải thiện độ chính xác trong kỹ thuật định vị ToA và AoA

a. Độ chính xác của kỹ thuật ToA, AoA

Có hai kỹ thuật định vị được ứng dụng rộng rãi là kỹ thuật tính toán thời gian đến của tín hiệu từ các trạm gốc phục vụ thiết bị di động (ToA) và kỹ thuật tính toán góc đến của tín hiệu từ các trạm gốc phục vụ thiết bị di động (AoA). Hai kỹ thuật này đều tính toán các tham số liên quan giữa trạm gốc (BTS/NodeB/eNodeB) và thiết bị di động (MS/UE/TE) để xác định vị vị trí của thiết bị di động. Các thuật toán được thực hiện để xác định vị trí (định vị) của thiết bị di động dùng hai kỹ thuật trên đã được nghiên cứu, công bố và có thể tìm thấy trên Internet. Tuy nhiên, trong quá trình ứng dụng các thuật toán đó để lập trình bài toán định vị, NCS thấy có nhiều nguyên

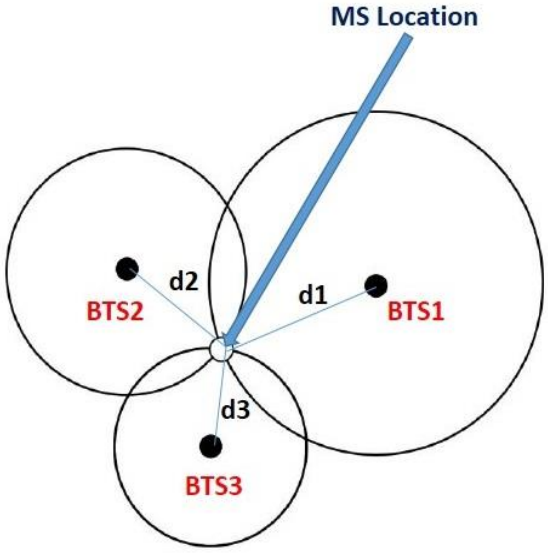
nhân khác nhau dẫn đến vị trí tính toán được trên hệ toạ độ địa lý (với không gian 3 chiều) là khó tính toán hoặc không chính xác. Bên cạnh đó, trong thực tế, do sai số của các phép đo nên bài toán định vị có thể tính toán ra nhiều kết quả, đặc biệt, với môi trường mạng di động hỗn hợp 2G, 3G, 4G-LTE như hiện nay. Do vậy, luận án đã nghiên cứu, phân tích để cải tiến, mở rộng thuật toán của kỹ thuật ToA và AoA nhằm cải thiện độ chính xác định vị.

b. Nguyên lý kỹ thuật và thuật toán gốc

Hai kỹ thuật định vị ToA và AoA đều lấy các tham số liên quan giữa trạm gốc và thiết bị di động để tính toán vị trí của thiết bị di động, trong đó, một tham số cơ sở là số nhận dạng của Cell di động (CellID – CID). Do vậy, hai kỹ thuật này có thể viết tắt là CID-ToA và CID-AoA.

Nguyên lý kỹ thuật định vị CID-ToA:

Giả sử thiết bị di động (MS/UE) có 3 trạm gốc (BTS/eNB) phục vụ và khoảng cách giữa các trạm gốc và thiết bị di động lần lượt là *d1, d2, d3* thì tọa độ của thiết bị di động được *x*ác định tại giao điểm của 3 vòng tròn có tâm tại các tọa độ của trạm gốc và có bán kính *d1, d2, d3*.

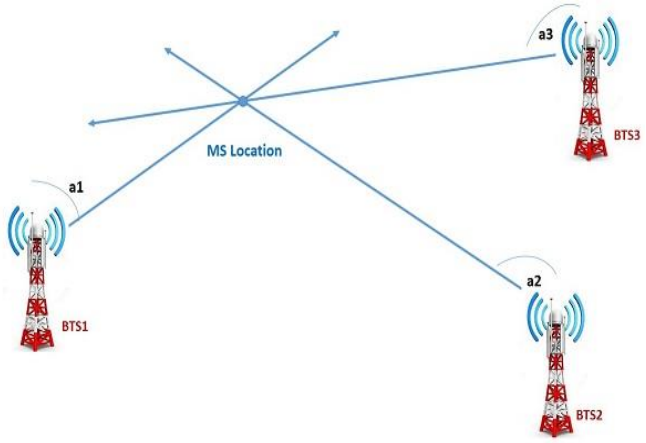


Hình 2. 1. Mô tả nguyên lý kỹ thuật định vị CID-ToA

Nguyên lý kỹ thuật định vị CID-AoA:

Giả sử thiết bị di động có 3 trạm gốc phục vụ và góc giữa 3 trạm gốc đến thiết bị di động lần lượt là *a1, a2, a3* thì tọa độ của thiết bị di động được xác định tại điểm

giao nhau của 3 vector có gốc tại các trạm gốc và hướng của chúng tạo với phương thẳng đứng các góc *a1*, *a2*, *a3*.



Hình 2. 2. Mô tả nguyên lý kỹ thuật định vị CID-AoA

Các nguyên lý kỹ thuật định vị nói trên chỉ tiếp cận vấn đề có tính chất tư tưởng giải thuật và lý thuyết, nguyên lý chung, mà không trình bày chi tiết từng bước cách xác định tọa độ của thiết bị di động và không bao giờ có một công thức chung tính toán, xác định tọa độ của thiết bị di động. Do đó, khi áp dụng các nguyên lý kỹ thuật định vị trên, cần nghiên cứu xây dựng một thuật toán xác định tọa độ của thiết bị di động một cách chính xác thì bài toán định vị mới có ý nghĩa.

Bản chất của thuật toán định vị nói trên chính là việc tính toán xác định tọa độ điểm cắt nhau của các vòng tròn trong hệ tọa độ địa lý (Geographic Coordinates), không gian 3 chiều (3D). Việc xác định tọa độ các điểm cắt nhau của các vòng tròn trong không gian 2 chiều thì dễ dàng thực hiện bằng toán học. Nhưng ở đây, bài toán cần thiết là tính toán trong hệ tọa độ địa lý với không gian 3 chiều. Nó sẽ có nhiều khó khăn và cần nghiên cứu, cải tiến để tìm ra thuật toán tối ưu.

Trong không gian 3 chiều cũng như hệ tọa độ địa lý, nếu các vòng tròn có bán kính bằng nhau, Google đã cung cấp hàm lập trình trên JavaScrip để xác định tọa độ điểm cắt nhau. Tuy nhiên, đối với trường hợp các vòng tròn có bán kính khác nhau thì hàm của Google không có kết quả và không sử dụng được. Để giải quyết bài toán tìm tọa độ điểm cắt nhau của các vòng tròn mà bán kính khác nhau trong hệ tọa độ địa lý, luận án đã tham khảo nhiều nguồn tài liệu trên Internet, nhưng cho kết quả không chính xác.

Nội dung dưới đây minh họa việc sử dụng một thuật toán công bố trên Internet cho việc xác định tọa độ điểm cắt nhau của các vòng tròn trong hệ tọa độ địa lý mà bán kính khác nhau đã cho kết quả không chính xác.

Nội dung thuật toán:

* **Đầu vào**:

- Vòng tròn thứ nhất: Tâm là điểm P1 = (lat_1/lon_1), bán kính *R1*.

- Vòng tròn thứ hai: Tâm là điểm P2 = (lat_2/lon_2), bán kính *R2*.

Trong đó lat_1/lon_1, lat_2/lon_2 lần lượt là vĩ độ/kinh độ của điểm P1, P2. Các bán kính của 2 vòng tròn *R1*, *R2* được đo dọc theo hình cầu, có đơn vị đo là hải lý (NM-nautical mile), là độ dài cung kinh tuyến tương ứng với 1’ (1/60 của 1 độ).

* **Đầu ra**: Tọa độ (vĩ độ/kinh độ) các điểm cắt nhau của 2 đường tròn trên bề mặt trái đất.

* **Thuật toán**:

- Bước 1. Chuyển đổi vĩ độ/kinh độ (*lat*/*lon*) của P1, P2 sang tọa độ địa tâm (là hệ tọa độ trong đó trái đất được mô hình hóa dưới dạng hình cầu trong không gian 3 chiều xyz, trục x chỉ kinh tuyến gốc, trục y chỉ hướng 90 độ trong mặt phẳng xích đạo, trục z chỉ hướng Bắc cực):

Giả sử $x_1 = (x_{11}, x_{12}, x_{13})$ và $x_2 = (x_{21}, x_{22}, x_{23})$ là tọa độ của các điểm P1, P2 trong hệ tọa độ địa tâm. Khi đó:

$x_{11} = \cos(lon_1)*\cos(lat_1)$

$x_{12} = \sin(lon_1)*\cos(lat_1)$

$x_{13} = \sin(lat_1)$

$x_{21} = \cos(lon_2)*\cos(lat_2)$

$x_{22} = \sin(lon_2)*\cos(lat_2)$

$x_{23} = \sin(lat_2)$

- Bước 2. Biến đổi bán kính *R1*, *R2* (được đo dọc hình cầu - đơn vị NM) sang dạng các góc r_1, r_2 (được đo dọc theo hình cầu - đơn vị radian).

r_1 = (*pi*/180)*(1/60)**R1* = 0.0002908888**R1* (radian);

r_2 = (*pi*/180)*(1/60)**R2* = 0.0002908888**R2* (radian).

- Bước 3. Xác định tọa độ điểm $\mathbf{x_0}$ nằm trên giao tuyến của 2 mặt phẳng chứa 2 đường tròn ban đầu, sao cho $\mathbf{x_0}$ là tổ hợp tuyến tính của $\mathbf{x_1}$ và $\mathbf{x_2}$ ($\mathbf{x_0}$ = *a*$\mathbf{x_1}$ + *b*$\mathbf{x_2}$).

+ Tính tích vô hướng của $\mathbf{x_1}$ và $\mathbf{x_2}$: $q = x_{11}*x_{21} + x_{12}*x_{22} + x_{13}*x_{23}$

+ Tính các hệ số *a*, *b*:

a = (cos(r_1) – cos(r_2)**q*)/(1-*q*^2)

b = (cos(r_2) – cos(r_1)**q*)/(1-*q*^2)

+ Tính $\mathbf{x_0}$ (có tọa độ địa tâm (x_{01}, x_{02}, x_{03}))

$\mathbf{x_0} = a*\mathbf{x_1} + b*\mathbf{x_2}$

$\mathbf{x_0} = a*(x_{11}, x_{12}, x_{13}) + b*(x_{21}, x_{22}, x_{23})$

$\mathbf{x_0} = (a*x_{11} + b*x_{21}, a*x_{12} + b*x_{22}, a*x_{13} + b*x_{23})$

Do đó:

$x_{01} = a*x_{11} + b*x_{21}$

$x_{02} = a*x_{12} + b*x_{22}$,

$x_{03} = a*x_{13} + b*x_{23}$).

- Bước 4. Xác định tích có hướng **n** (có tọa độ địa tâm (n_1, n_2, n_3) của $\mathbf{x_1}$ và $\mathbf{x_2}$: $\mathbf{n} = \mathbf{x_1} \sim \text{Cross} \sim \mathbf{x_2}$

$\mathbf{n} = (x_{12}*x_{23} - x_{13}*x_{22}, x_{13}*x_{21} - x_{11}*x_{23}, x_{11}*x_{22} - x_{12}*x_{21})$

Do đó:

$n_1 = x_{12}*x_{23} - x_{13}*x_{22}$

$n_2 = x_{13}*x_{21} - x_{11}*x_{23}$

$n_3 = x_{11}*x_{22} - x_{12}*x_{21}$.

- Bước 5. Tìm 2 điểm cắt nhau C1, C2 của 2 đường tròn có dạng $\mathbf{x_0} + t^*\mathbf{n}$ nằm trên bề mặt trái đất, độ dài của chúng bằng 1.

Có 2 tham số *t* thỏa mãn:

t_1 = + sqrt ((1- $\mathbf{x_0} . \mathbf{x_0}$)/**n**.**n**)

t_2 = - sqrt ((1- $\mathbf{x_0} . \mathbf{x_0}$)/**n**.**n**)

Trong đó $\mathbf{x_0} . \mathbf{x_0}$ là tích vô hướng của $\mathbf{x_0}$ và chính nó, **n**.**n** là tích vô hướng của **n** và chính nó, được xác định như sau:

$\mathbf{x_0} . \mathbf{x_0} = x_{01} * x_{01} + x_{02} * x_{02} + x_{03} * x_{03}$

$\mathbf{n}.\mathbf{n} = n_1 * n_1 + n_2 * n_2 + n_3 * n_3$

Khi đó:

C1 có tọa độ địa tâm: $\mathbf{c_1} = \mathbf{x_0} + t_1 * \mathbf{n} = (x_{01} + t_1 * n_1,\ x_{02} + t_1 * n_2,\ x_{03} + t_1 * n_3)$

C1 có tọa độ địa tâm: $\mathbf{c_2} = \mathbf{x_0} + t_2 * \mathbf{n} = (x_{01} + t_2 * n_1,\ x_{02} + t_2 * n_2,\ x_{03} + t_2 * n_3)$

- Bước 6. Biến đổi các kết quả tìm được trở lại dạng (lat/lon) bằng cách chuyển tọa độ địa tâm sang tọa độ có vĩ độ và kinh độ bằng công thức sau:

Lon(C1) = ArcTan{($x_{02} + t_1 * n_2$)/($x_{01} + t_1 * n_1$)}

Lat(C1) = ArcTan{($x_{03} + t_1 * n_3$)/sqrt([$x_{01} + t_1 * n_1$]^2 + [$x_{02} + t_1 * n_2$]^2)}

Lon(C2) = ArcTan{($x_{02} + t_2 * n_2$)/($x_{01} + t_2 * n_1$)}

Lat(C2) = ArcTan{($x_{03} + t_2 * n_3$)/sqrt([$x_{01} + t_2 * n_1$]^2 + [$x_{02} + t_2 * n_2$]^2])}

Cuối cùng ta chuyển đơn vị đo vĩ độ/kinh độ của các điểm cắt nhau giữa 2 đường tròn vừa tìm được trên đây từ radian sang độ.

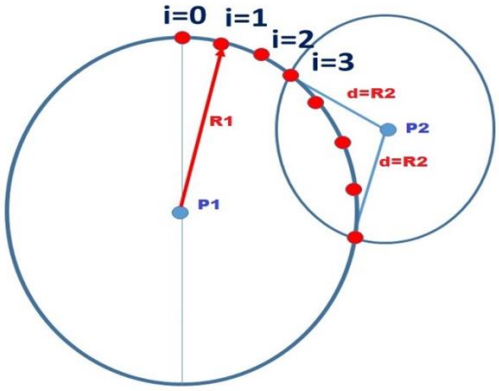
Dựa vào thuật toán trên, luận án đã lập trình trên ngôn ngữ Rcode để kiểm chứng tính chính xác. *(Kết quả kiểm chứng sẽ được trình bày trong Chương 4).*

Rcode chạy thông suốt nhưng cho kết quả tọa độ 2 điểm cắt nhau khi biểu diễn trên bản đồ thì không chính xác. Ngoài ra luận án cũng tham khảo nhiều tài liệu khác trong việc xác định tọa độ điểm cắt nhau của các vòng tròn trong không gian 3 chiều mà bán kính khác nhau cũng không có kết quả. Từ đó, vấn đề khó khăn nhất là cần

tự nghiên cứu thuật toán xác định tọa độ điểm cắt nhau của 2 vòng tròn trong hệ tọa độ địa lý mà bán kính khác nhau.

c. Cải tiến thuật toán

Thuật toán cải tiến được mô tả như sau:



Hình 2. 3. Mô tả thuật toán xác định tọa độ điểm cắt nhau của hai vòng tròn trong hệ tọa độ địa lý

Trong hệ tọa độ địa lý, cho 2 vòng tròn có tâm tại P1 và P2 và bán kính lần lượt là *R1*, *R2*. Giả sử 2 vòng tròn cắt nhau tại 2 điểm, ta cần xác định tọa độ của 2 điểm cắt nhau này. Tại tâm của 1 trong 2 vòng tròn, giả sử tại P1, ta có một vector và độ dài vector bằng bán kính *R1*, ta sẽ cho vector quay quanh tâm P1, với mỗi bước nhảy Ɛ dương, đủ nhỏ, ở đây ta chọn Ɛ=0.1, như thế, sau mỗi bước nhảy, sẽ có một điểm trên vòng tròn là điểm dừng của vector, đó chính là các điểm *i*=0, *i*=1, *i*=2…v.v.

Tại mỗi điểm dừng thứ i, ta hãy kiểm tra khoảng cách từ tọa độ của điểm i đến tâm của vòng tròn còn lại, đó chính là P2, giả sử khoảng cách đó là *d* và bằng *R2*, khi đó, tọa độ của i chính là tọa độ của điểm cắt nhau thứ nhất. Trên hình minh họa, tại điểm *i*=3, ta có *d=R2*, do đó, tọa độ tại *i*=3 chính là tọa độ của điểm cắt nhau thứ nhất. Sau đó, vector tiếp tục quay và quá trình kiểm tra *d=R2* lại tiếp tục. Đến *i*=7, ta lại có *d=R2*, khi đó tọa độ *i*=7 chính là tọa độ của điểm cắt nhau thứ 2.

Sau đây là code giả mã để minh họa thuật toán nói trên:

i=0;

alpha=0;(alpla là góc quay)

Ɛ=0.1

While (alpha<360)

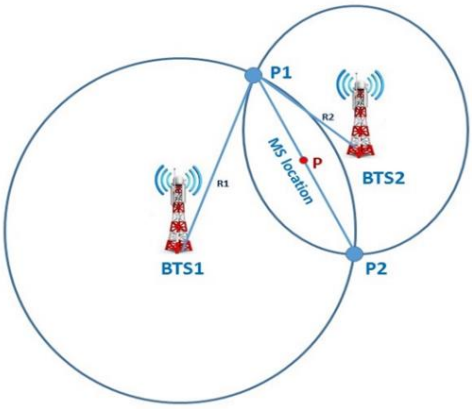
```
{
Pi= coordinate(R1,alpha);
d= distance(Pi,P2)
if(d=R2)
    {
       Intersection =Pi
if   (getIntersectionPoint(1) == null)
getIntersectionPoint(1) =Pi
else
getIntersectionPoint(2) =Pi
}
else
 {
i =i + 1;
                alpha=i*Ɛ;
}
```

Kết quả chạy chương trình đã tính toán chính xác tọa độ 2 điểm cắt nhau của 2 vòng tròn bán kính khác nhau trong hệ tọa độ địa lý *(So sánh kết quả định vị trước và sau khi cải tiến thuật toán được trình bày trong Chương 4).*

d. Mở rộng thuật toán

Trên đây, luận án đã trình bày việc cải tiến thuật toán để xác định tọa độ điểm cắt nhau của các vòng tròn trong hệ tọa độ địa lý mà bán kính khác nhau. Theo nguyên lý kỹ thuật định vị, điểm cắt nhau của 3 vòng tròn chính là tọa độ của thiết bị di động. Đây là một trường hợp đặc biệt, khi mà thiết bị di động ở đúng vị trí của 3 vòng tròn cắt nhau. Trong thực tế, do sai số của phép đo mà các vòng tròn thường cắt nhau tại nhiều điểm. Do đó, để xác định tọa độ của thiết bị di động ta cần xác định tọa độ của tất cả các điểm cắt nhau, sau đó, vị trí của thiết bị di động sẽ được xác định nằm trong vùng tạo bởi các điểm cắt nhau. Được chia thành 2 trường hợp:

(1) Trường hợp chỉ có 2 trạm gốc và 2 vòng tròn cắt nhau tại 2 điểm:



Hình 2. 4. Trường hợp chỉ có 2 trạm gốc và 2 vòng tròn cắt nhau tại 2 điểm

Trong trường hợp này, tọa độ của thiết bị di động nhiều khả năng ở tại điểm P là trung điểm của đoạn thẳng P1P2. Ta cần nghiên cứu tính tọa độ điểm P (trong hệ tọa độ địa lý). Sau đây là thuật toán mở rộng theo các bước tính toán sau:

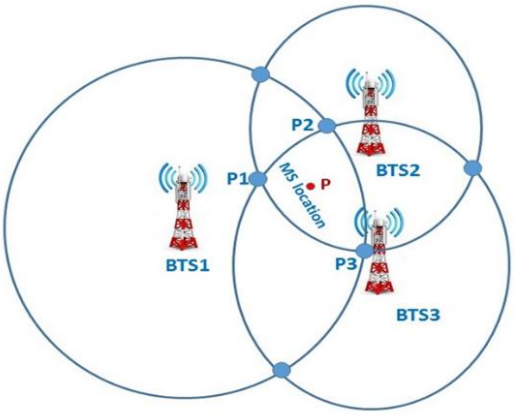
- Tính góc *b* (bearing) giữa hai tọa độ địa lý P1 và P2.

- Tính khoảng cách *d* là khoảng cách trung bình giữa 2 tọa độ P1 và P2.

- Sau khi tính được góc *b* và *d* tính tọa độ điểm P cho bởi tọa độ P1 và các giá trị *b* và *d*.

Tọa độ điểm P nhận được chính là tọa độ thiết bị di động.

(2) Trường hợp có nhiều trạm gốc hơn (có nhiều hơn 2 vòng tròn) và chúng cắt nhau tại nhiều điểm:



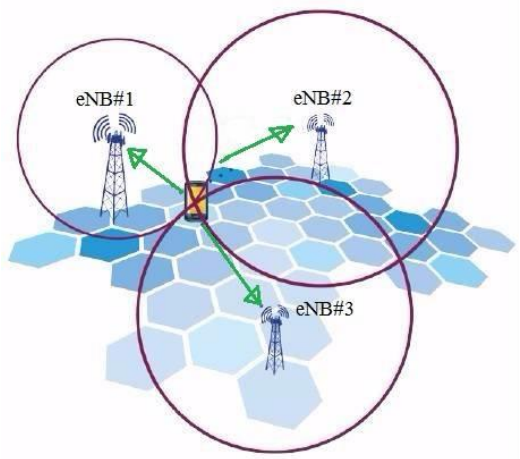
Hình 2. 5. Mô tả trường hợp 3 vòng tròn cắt nhau tại nhiều điểm

Trong trường hợp này, cần tính tọa độ của tất cả các điểm cắt nhau và xác định vùng giao nhau của 3 vòng tròn, ở đây là vùng tạo bởi 3 điểm P1, P2, P3 và tọa độ của thiết bị di động sẽ nằm ở giữa vùng giao này (điểm P) [J2; 27-29].

2.2.4. Giải pháp kỹ thuật U-TDoA nâng cao độ khả dụng và chính xác định vị

Trong nguyên lý kỹ thuật định vị ToA, một trong những kỹ thuật thường được sử dụng để nâng cao tính khả dụng và độ chính xác định vị là U-TDoA. U-TDoA sử dụng nguyên lý tính toán chênh lệch thời gian đường lên bởi nhiều trạm gốc (BTS/eNB) để xác định vị trí của thiết bị di động (MS/UE). Các máy thu độ nhạy cao của các trạm gốc sẽ thu nhận tín hiệu đường lên từ thiết bị di động đến trạm gốc. Phép tính toán sẽ lấy sự chênh lệch thời gian đường lên của tín hiệu từ nhiều trạm gốc khác nhau để tính toán. Do vị trí của trạm gốc là cố định lên phép tính toán này sẽ ước tính được vị trí của thiết bị di động.

Nguyên lý hoạt động của kỹ thuật U-TDoA được mô tả như hình vẽ sau:



Hình 2. 6. Mô tả nguyên lý kỹ thuật U-TDoA

Kỹ thuật U-TDoA được ứng dụng rộng rãi trong các tình huống khẩn cấp, tìm kiếm cứu hộ cứu nạn, giám sát an ninh công cộng bởi các đặc điểm vượt trội về độ khả dụng và độ chính xác của nó. Bảng sau đây mô tả đặc điểm và ứng dụng của kỹ thuật U-TDoA:

Bảng 2. 3. Đặc điểm và ứng dụng của U-TDoA

TT	Mô tả	Đặc điểm, ứng dụng
1.	Nguyên lý	Nguyên lý kỹ thuật định vị tính toán thời gian đến của tín hiệu (ToA), trong đó sử dụng chênh lệch thời gian đến của tín hiệu đường lên từ thiết bị di động (MS/UE) bởi nhiều trạm gốc (BTS/eNB) để ước lượng vị trí thiết bị di động.
2.	Độ khả dụng và độ chính xác	Do U-TDoA sử dụng máy thu độ nhạy cao của trạm gốc, nên có thể thu nhận được tín hiệu đường lên từ thiết bị di động ngay cả khi xuyên qua các tòa nhà (tức thiết bị di động ở trong nhà), không bị ảnh hưởng bởi các vật

TT	Mô tả	Đặc điểm, ứng dụng
		thể che chắn thường gặp như cây cối, công trình xây dựng che chắn tầm nhìn thẳng. Do đặc điểm trên, sử dụng định vị U-TDoA có độ khả dụng và chính xác hơn nhiều so với định vị sử dụng GPS của máy di động. *(Kỹ thuật sử dụng GPS của máy di động đòi hỏi máy di động phải ở trong tầm nhìn thẳng (LOS) với các vệ tinh GPS. Nếu máy di động ở bên trong các tòa nhà hoặc ở những nơi xung quanh có nhiều tòa nhà cao tầng thì tín hiệu vệ tinh GPS sẽ yếu hoặc không thể đến được máy di động. Mặt khác, tín hiệu vệ tinh GPS cũng sẽ yếu khi máy di động ở những khu vực có nhiều cây cối như rừng rậm. Những tình huống khó khăn này thường xảy ra như tìm kiếm cứu hộ cứu nạn trong các tòa nhà hay trong rừng núi).*
3.	Ứng dụng	U-TDoA hiệu quả cho các tính huống khẩn cấp như tìm kiếm cứu hộ cứu nạn, các ứng dụng giám sát an ninh công cộng.

[3, 23-29].

2.3. Nhận xét, đánh giá về giải pháp kỹ thuật được đề xuất

2.3.1. Hiệu quả của giải pháp

Kết quả nghiên cứu trên đã xác định được giải pháp kỹ thuật "Hệ thống định vị lai ghép tiên tiến" trên cơ sở kết hợp đa dạng nguồn dữ liệu, cải thiện độ chính xác, nâng cao độ khả dụng để nâng cao hiệu quả định vị thiết bị di động 4G. Hiệu quả của giải pháp kỹ thuật sẽ thể hiện ở các đặc thù sau, hoạt động phù hợp trên nền mạng 4G nói chung và mạng 4G Việt Nam nói riêng:

(1) Tăng độ khả dụng, hữu ích:

Với cơ sở dữ liệu đã được tiếp nhận, làm giàu với da dạng nguồn dữ liệu định vị đầu vào (như dữ liệu vị trí từ nhà mạng, dữ liệu vị trí từ máy cầm tay, dữ liệu vị trí từ các thiết bị định vị cơ động, thiết bị thu thập tham số IMSI/IMEI …) cùng với các dữ liệu tham chiếu (dữ liệu giao thông, dữ liệu môi trường mạng Internet/Wifi…), hệ thống sẽ phân lớp, xác định được chính xác đối tượng cần định vị, áp dụng được thuật toán, kỹ thuật phù hợp hoặc lai ghép nhiều thuật toán, kỹ thuật để định vị được đối tượng đó. Trong trường hợp nguồn dữ liệu đầu vào nào đó không khả dụng, hệ thống

sẽ tìm kiếm từ nguồn dữ liệu khác để tính toán kết quả. Hoặc hệ thống sẽ tập hợp nhiều nguồn dữ liệu một lúc, áp dụng nguyên lý định vị lai ghép để tính toán kết quả. Trong trường hợp, tại thời điểm nào đó không có nguồn dữ liệu đầu vào nào là khả dụng, hệ thống áp dụng các công nghệ tiên tiến để tìm kiếm, xác định vị trí ngay trước đó hay trong lịch sử từ dữ liệu được lưu trữ. Bởi sử dụng nền tảng cơ sở dữ liệu mở, đa nguồn, hệ thống sẵn sàng bổ sung nhiều tính năng cần thiết, hữu ích khác ngoài tính năng định vị, như hiển thị, truy vết đường đi trên bản đồ số; phân tích mối quan hệ của đối tượng theo thực thể; tổng hợp số liệu, trích xuất báo cáo phục vụ thông tin chỉ huy v.v…

(2) Cải thiện độ chính xác:

Với kỹ thuật định vị lai ghép cùng cơ sở dữ liệu định vị đã được thu thập làm giàu, tiếp nhận thông tin từ nhiều nguồn dữ liệu định vị đầu vào khác nhau và các dữ liệu tham chiếu, cùng với khả năng áp dụng các công nghệ mới như học máy, trí tuệ nhân tạo, các thuật toán định vị sẽ được cải tiến, mở rộng liên tục, độ chính xác định vị sẽ được cải thiện hơn so với các giải pháp định vị truyền thống.

(3) Đáp ứng yêu cầu thực tiễn của cơ quan an ninh trong thực trạng mạng di động hiện nay:

Thực trạng mạng di động hiện có nhiều nhà cung cấp, đa dạng dịch vụ, hỗn hợp công nghệ 2G/3G/4G và chưa có khả năng cung cấp nhiều loại dữ liệu cần thiết cho định vị, giải pháp kỹ thuật lai ghép tiên tiến cho phép CQAN tận dụng được các nguồn lực từ nhiều nguồn dữ liệu khác nhau, từ các hệ thống đã có để giải quyết yêu cầu định vị.

(4) Nền tảng cho áp dụng công nghệ mới và sẵn sàng nâng cấp, mở rộng trong tương lai:

Cơ sở dữ liệu định vị được xây dựng trên nền tảng dữ liệu mở với đa dạng nguồn dữ liệu đầu vào cho phép hệ thống sẵn sàng tiếp nhận thêm nguồn dữ liệu công nghệ di động mới như 5G cũng như dữ liệu tham chiếu liên quan. Các thuật toán, phần mềm ứng dụng (API) được xây dựng từ nguồn mở và lai ghép nhiều nguyên lý kỹ thuật định vị khác nhau cho phép sẵn sàng mở rộng, bổ sung áp dụng các kỹ thuật

định vị mới. Hệ thống cũng sẽ cho phép tích hợp với các hệ thống kỹ thuật khác thành một trung tâm xử lý dữ liệu tổng thể.

Qua nghiên cứu tổng hợp và dữ liệu thực nghiệm, có thể đánh giá một số hiệu quả của giải pháp được đề xuất qua một số thông tin định lượng sau:

- Cải thiện độ chính xác định vị ToA, AoA: sai số kết quả tính toán vị trí và biểu diễn trên bản đồ số có thể đến 0 mét sau khi cải tiến thuật toán định vị CID-ToA, CID-AoA so với gần 50 mét khi sử dụng thuật toán gốc. *(Chi tiết có trong Bảng 4.1. Bảng so sánh kết quả kiểm thử cải tiến thuật toán định vị).*
- Nâng cao hiệu quả định vị bằng ứng dụng kỹ thuật U-TDoA:

Luận án đề xuất sử dụng kỹ thuật định vị U-TDOA trong các trường hợp định vị hỗ trợ tìm kiếm cứu hộ, cứu nạn. Trong trường hợp này, việc sử dụng U-TDOA vượt trội sử dụng GPS về độ khả dụng và độ chính xác, như trình bày cụ thể ở bảng 2.3 ở trên.

2.3.2. Khuyến nghị

Việc sử dụng "Hệ thống định vị lai ghép tiên tiến" cần lưu ý các vấn đề sau:

- Trong hệ thống định vị lai ghép, mỗi nguyên lý kỹ thuật sẽ có ưu, nhược điểm khác nhau. Bên cạnh đó, trong thực tế, một hệ thống định vị lai ghép khi xử lý định vị một thiết bị di động 4G sẽ có nhiều nguyên nhân dẫn tới kết quả tính toán vị trí không chính xác hoặc đưa ra nhiều kết quả vị trí. Do vậy, luôn cần thiết phải nghiên cứu cải tiến, mở rộng các nguyên lý kỹ thuật định vị có sẵn để lập trình được API ứng dụng có kết quả ngày càng chính xác hơn.

- Cần tăng cường thu thập và làm giàu dữ liệu định vị từ nhiều nguồn khác nhau, tiến tới thiết lập được cơ sở dữ liệu lớn, áp dụng được các công nghệ trí tuệ nhân tạo, học máy để nâng cao tính khả dụng và độ chính xác định vị.

2.4. Kết luận Chương 2

Chương 2 của luận án đã trình bày nghiên cứu về giải pháp kỹ thuật tổng thể cho định vị thiết bị di động thế hệ thứ tư. Giải pháp kỹ thuật tổng thể được tóm tắt như sau:

- Sử dụng giải pháp kỹ thuật "Hệ thống định vị lai ghép tiên tiến" trên cơ sở thu thập, kết hợp xử lý đa dạng nguồn dữ liệu để nâng cao hiệu quả định vị thiết bị di động.

- Cải thiện độ chính xác định vị trên cơ sở cải tiến, mở rộng thuật toán kỹ thuật định vị cơ sở ToA, AoA. Cải thiện độ khả dụng và độ chính xác định vị bằng cách sử dụng kỹ thuật định vị U-TDoA.

Do yêu cầu của bài toán định vị thiết bị di động thế hệ thứ tư cần thu thập, lưu trữ, làm giàu, tích lũy một cơ sở dữ liệu định vị lớn từ đa dạng các nguồn thông tin, giải pháp đã đề xuất xây dựng cơ sở dữ liệu định vị đa nguồn trên nền tảng dữ liệu mở. Một cơ sở dữ liệu lớn trên nền tảng dữ liệu mở sẽ đáp ứng yêu cầu thu thập, xử lý đa dạng dữ liệu từ nhiều nguồn, nhiều định dạng khác nhau. Cơ sở dữ liệu lớn này đồng thời sẽ cho phép áp dụng các công nghệ xử lý dữ liệu mới như đồ thị tri thức, học máy, trí tuệ nhân tạo để nâng cao hiệu quả định vị thiết bị di động.

CHƯƠNG 3. MÔ HÌNH HỆ THỐNG KỸ THUẬT ĐỊNH VỊ THIẾT BỊ DI ĐỘNG VÀ ỨNG DỤNG CHO CÔNG TÁC AN NINH

Căn cứ vào giải pháp kỹ thuật định vị đã đề xuất, nội dung Chương 3 sau đây trình bày nghiên cứu xây dựng mô hình tổng thể hệ thống kỹ thuật định vị thiết bị di động và ứng dụng cho công tác an ninh.

3.1. Mô hình kiến trúc tổng thể hệ thống định vị thiết bị di động

3.1.1. Mô hình kiến trúc hệ thống

Với yêu cầu ứng dụng giải pháp hệ thống định vị lai ghép tiên tiến trên cơ sở kết hợp đa dạng nguồn dữ liệu nhằm nâng cao hiệu quả định vị thiết bị di động và cung cấp đa dạng dữ liệu cho các đầu ra khác nhau, luận án đề xuất xây dựng hệ thống định vị thiết bị di động sử dụng phân lớp định vị, bảo mật và trạm gốc giả lập ứng dụng cho công tác an ninh với mô hình kiến trúc tổng thể như hình 3.1.

Hình 3. 1. Sơ đồ kiến trúc tổng thể hệ thống định vị

3.1.2. Mô tả kiến trúc hệ thống

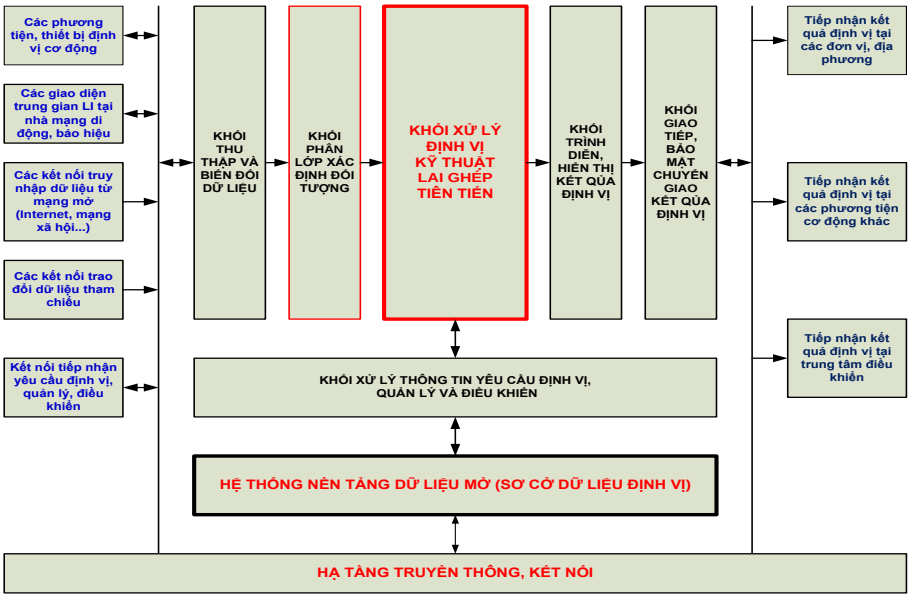
Mô hình kiến trúc tổng thể hệ thống định vị thiết bị di động được chia thành 4 thành phần: đầu vào dữ liệu; trung tâm xử lý định vị; đầu ra kết quả định vị; tiếp nhận yêu cầu định vị, quản lý và điều khiển. Thành phần đầu vào dữ liệu sẽ tiếp nhận, thu thập đa dạng dữ liệu định vị từ các nguồn khác nhau. Thành phần trung tâm xử lý định vị là hệ thống định vị lai ghép tiên tiến trên cơ sở kết hợp xử lý đa dạng, đa nguồn dữ liệu đầu vào; kết hợp và cải tiến các thuật toán định vị khác nhau; phân lớp

xác định đối tượng; bảo mật chuyển giao kết quả định vị và trạm gốc giả lập thu thập tham số IMSI/IMEI. Thành phần đầu ra kết quả định vị sẽ có nhiều đầu ra, cung cấp kết quả định vị cho các mục đích sử dụng khác nhau. Thành phần tiếp nhận yêu cầu định vị, quản lý và điều khiển hệ thống sẽ tiếp nhận yêu cầu định vị từ người sử dụng yêu cầu, thực hiện các chức năng quản lý và điều khiển hệ thống.

3.2. Cấu trúc, chức năng hệ thống định vị thiết bị di động

3.2.1. Sơ đồ khối cấu trúc hệ thống

Hệ thống định vị thiết bị di động theo mô hình kiến trúc tổng thể được đề xuất ở trên bao gồm các khối chức năng cụ thể như sơ đồ cấu trúc sau:



Hình 3. 2. Sơ đồ cấu trúc chức năng hệ thống định vị

3.2.2. Mô tả cấu trúc, chức năng hệ thống

3.2.2.1. Các khối đầu vào dữ liệu định vị

Đầu vào dữ liệu định vị thu thập từ đa dạng các nguồn dữ liệu sau:

- Các phương tiện, thiết bị định vị cơ động (như các thiết bị thu thập thông tin BTS/eNB tự động, thiết bị giả lập trạm gốc thu thập tham số IMSI/IMEI, thiết bị định vị cơ động, thiết bị khoanh vùng định vị v.v…).

- Các giao diện trung gian thu chặn hợp pháp (LI) tại các nhà mạng di động, mạng báo hiệu SS7.

Các giao diện trung gian này sẽ thu thập dữ liệu định vị trực tuyến từ các mạng di động được phép kết nối và các công cụ giám sát trên từ nền tảng các mạng thông tin di động (ví dụ đường kết nối online từ điểm báo hiệu số 7, đường kết nối online từ máy chủ định vị của nhà mạng di động v.v…) và từ các cơ sở dữ liệu offline được cung cấp (như dữ liệu list cuộc gọi, dữ liệu BTS/eNB cập nhật theo thời gian).

- Các kết nối truy nhập dữ liệu từ mạng mở (Internet, mạng xã hội …).

Các kết nối này thu thập dữ liệu từ nguồn mở như dữ liệu OpenCellID, dữ liệu Cell-ID từ Google, dữ liệu Wifi Hotspot được cung cấp từ một số nhà cung cấp cộng đồng trên thế giới, dữ liệu bản đồ số Google Maps v.v…cũng như dữ liệu môi trường mạng mà thiết bị di động có thể, đã, đang và sẽ truy cập như địa chỉ IP, địa chỉ MAC kết nối, thông tin đăng ký hoặc xác thực định danh người dùng, các dữ liệu thực thể khác liên quan đến đối tượng như hình ảnh, video, bạn bè, nhóm v.v…

- Các kết nối trao đổi dữ liệu tham chiếu từ cơ sở dữ liệu liên quan đến đối tượng như dữ liệu giao thông, dữ liệu môi trường mạng, dữ liệu media v.v…

Các dữ liệu trên bao gồm cả loại có cấu trúc và loại phi cấu trúc, trực tuyến hoặc không trực tuyến, dữ liệu thô hoặc dữ liệu đã được xử lý.

3.2.2.2. Khối đầu vào yêu cầu định vị, quản lý và điều khiển hệ thống

Kết nối tiếp nhận các yêu cầu định vị, các tác vụ quản lý và điều khiển hệ thống, các yêu cầu này có thể trực tiếp tại trung tâm định vị bởi người quản lý, điều khiển hay từ xa bởi các người dùng được phân quyền.

3.2.2.3. Trung tâm định vị

Trung tâm định vị là một hệ thống kỹ thuật bao gồm các khối chức năng chính sau:

- Hạ tầng truyền thông, kết nối cho nội bộ trung tâm và các kết nối đến đầu vào dữ liệu, đầu vào quản lý, điều khiển; đầu ra kết quả định vị.
- Hệ thống nền tảng dữ liệu mở (cơ sở dữ liệu định vị) bao gồm các thiết bị máy chủ, lưu trữ cũng như các phần mềm hệ điều hành, phần mềm điều khiển lưu trữ; hình thành hệ thống cơ sở dữ liệu lớn trên nền tảng mở phục vụ toàn bộ hệ thống.
- Khối xử lý thông tin từ các yêu cầu định vị, các tác vụ quản lý, điều khiển hệ thống.

- Khối xử lý kỹ thuật định vị lai ghép tiên tiến bao gồm các giao diện lập trình ứng dụng khác nhau, lai ghép các kỹ thuật định vị khác nhau để xử lý dữ liệu và cho ra kết quả định vị.

- Khối thu thập và biến đổi dữ liệu đầu vào đa nguồn có nhiệm vụ chuyển đổi các dữ liệu đa nguồn, đa dạng thành dữ liệu có nghĩa, phù hợp với định dạng mà các API xử lý kỹ thuật định vị cần thiết.

- Khối phân lớp xác định đối tượng có nhiệm vụ phân loại, xác định các tập đối tượng hoặc đối tượng định vị từ một loạt các dữ liệu thu thập được và từ yêu cầu định vị để khối xử lý trung tâm thực hiện định vị đối tượng đó.

- Khối trình diễn, hiển thị kết quả định vị lấy dữ liệu định vị của khối trung tâm, trình diễn nó trên các hình thức có nghĩa như số liệu tọa độ, vị trí trên bản đồ số, đồ thị mối quan hệ (ví dụ đồ thị mối quan hệ các số điện thoại gọi đi, đến), các mô tả thực thể liên quan (ví dụ một vị trí đối tượng di động đã được định vị trên bản đồ số, có hiển thị kinh độ, vĩ độ, các tham số trạm gốc phục vụ (Cell-LAC, Cell-ID) cùng với hình ảnh địa điểm địa lý nếu có; bản đồ truy vết đường đi (ví dụ bản đồ hiển thị đường đi của đối tượng qua truy vết định vị theo thời gian).

- Khối giao tiếp, bảo mật chuyển giao kết quả định vị. Các kết quả định vị, dù là số liệu đơn giản hay số liệu đã được trình diễn nêu trên cần được bảo mật và chuyển đến đầu ra bởi các giao tiếp kết nối khác nhau.

Đầu ra kết quả định vị sẽ được gửi đến thiết bị xử lý (máy tính, điện thoại…) ở xa; các thiết bị cơ động ở xa hoặc người dùng tại trung tâm điều khiển xử lý cho các mục đích khác nhau. Ví dụ, kết quả định vị sơ bộ (mức Cell-ID) và một số thông tin liên quan đến Cell đang phục vụ sẽ được gửi đến một xe cơ động ở xa để tìm hướng, định vị chính xác đối tượng.

3.3. Phân lớp, xác định đối tượng

Theo logic lý thuyết toán học, nếu cần tìm một đối tượng trong hàng loạt đối tượng thì trước tiên phải phân loại các đối tượng thành các lớp, và tiếp tục tìm kiếm trong lớp đó đối tượng đáng ngờ có đặc trưng gần nhất và sau đó là tìm kiếm mối liên quan của các đặc trưng đó với nhau và với các đối tượng khác thì sẽ xác định được

ngày càng chính xác đối tượng đó. Điều này là phù hợp với việc tìm kiếm, xác định một đối tượng định vị hoạt động đa dịch vụ trên môi trường di động 4G. Nghiên cứu sau đây sẽ xác định phương pháp phân lớp xác định đối tượng.

3.3.1. Bài toán lý thuyết phân lớp

Để xác định một đối tượng trong hàng loạt đối tượng, ta cần phải phân hoạch (Partition) tập tất cả đối tượng thành *k* lớp sao cho các đối tượng có các đặc trưng gần gũi nhất sẽ được cho vào một lớp. Như vậy để phân hoạch tốt, trước hết ta phải xây dựng độ đo giữa các đối tượng và độ độ đo giữa một phần tử với một lớp các đối tượng đối với số lớp *k* đã biết và số lớp *k* chưa biết. Một cách tổng quát bài toán được đặt ra như sau:

Cho X là một tập hợp hữu hạn khác rỗng tùy ý. Hãy phân hoạch X thành *k* tập hợp con $A_1, A_2, \ldots, A_k$ khác rỗng sao cho thỏa mãn các tiên đề sau đây:

Tiên đề 1. $A_i \cap A_j = \varnothing$, $i \neq j$, $i, j = 1, 2, \ldots, k$

Tiên đề 2. $A_1 \cup A_2 \cup \ldots \cup A_k = X$ và sao cho xác suất sai sót trong phân hoạch là bé nhất có thể.

Để giải quyết bài toán trên, luận án đã nghiên cứu hai lý thuyết phân lớp liên quan đến định vị, phân loại, xác định đối tượng, một là phân lớp có giám sát và phân lớp không có giám sát.

3.3.2. Phương pháp phân lớp, xác định đối tượng định vị

3.3.2.1. Yêu cầu

Để định vị một đối tượng, trước tiên chúng ta cần xác định đối tượng đó để có thể áp dụng được nguyên lý kỹ thuật định vị hiệu quả. Đối tượng ở đây được qui đồng là một thiết bị di động (MS/UE). Việc xác định đối tượng cần thực hiện theo mô hình 3 bước: thu thập thông tin về đối tượng và các thông tin liên quan; phân loại đối tượng; xác định đối tượng. Việc thu thập thông tin nhằm trả lời các câu hỏi ai, làm gì, ở đâu… cùng các đặc tính của nó như đặc điểm về người và các mối quan hệ. Trong bài toán định vị thì mối quan hệ quan trọng nhất cần xác định chính là các mối

liên lạc, ví dụ số thuê bao/ máy điện thoại sử dụng, địa chỉ IP truy cập Internet, liên lạc với ai, liên lạc từ đâu v.v… Đó chính là thu thập thông tin về "thực thể". Từ thực thể đó sẽ có nhiều cơ hội để tìm kiếm, xác định một đối tượng. Sau khi thu thập được hàng loạt thông tin và trong cơ sở dữ liệu hàng loạt đối tượng, làm thế nào để xác định chính xác một đối tượng, hay một MS/UE để tiến hành định vị. Nghiên cứu sau đây sẽ phân tích, giải quyết bài toán đó trên cơ sở hai bước: phân lớp đối tượng và xác định đối tượng.

3.3.2.2. Phương pháp phân lớp đối tượng

Để phân lớp đối tượng, ta cần dựa vào các đặc trưng của chúng. Bài toán phân lớp có giám sát được mô tả như sau: Cho trước một tập hợp hữu hạn Ω các đối tượng, mỗi đối tượng gồm n đặc trưng. Như vậy ta có thể coi Ω là một tập con trong không gian Euclide *n*-chiều R^n. Giả sử trên cơ sở thông tin nào đó ta có đối tượng $y \in R^n$. Để xác định y có trong tập hợp Ω hay không, bài toán thực hiện là hãy xác định xem có tồn tại một $x \in \Omega$ mà $y = x$ hay không? (Ở đây, ta hiểu khái niệm "$y = x$" theo nghĩa xác suất).

Để rõ hơn vấn đề này, ta xét bài toán phân lớp tổng quát nhất như sau:

Cho một tập hợp Ω hữu hạn tùy ý. Mỗi $x \in \Omega$ được gọi là một đối tượng (object) hay về mặt toán học, *x* được gọi là một phần tử (element) trong tập hợp Ω. Mỗi phần tử được thể hiện bởi các đặc trưng (characteristic) của nó. Như vậy, các phần tử khác nhau sẽ có các đặc trưng tương ứng không giống nhau. Để dễ dàng cho việc xây dựng phương pháp phân lớp (classification) các đối tượng của Ω, ta giả sử mỗi đối tượng được mô tả bởi *n* đặc trưng. Như vậy, ta có thể xem Ω như là một tập hợp con trong không gian Euclide *n* chiều (được ký hiệu là R^n) tức là $\Omega \subset R^n$. Bài toán đặt ra là hãy phân hoạch Ω thành *k* lớp: $A_1, A_2, \ldots, A_k$ với $A_i \neq \varnothing$, $i = 1, 2, \ldots, k$ sao cho:

i/ $A_i \cap A_j = \varnothing$, $i \neq j$, $i, j = 1, 2, \ldots, k$

ii/ $\bigcup_{i=1}^{k} A_i = \Omega$

Rõ ràng là có nhiều cách phân hoạch (partition) Ω thỏa mãn các điều kiện đã nêu. Song, dù phân hoạch bằng cách nào cũng đều xảy ra hai trường hợp:

Trường hợp 1: Đối tượng $x \in \Omega$, thực tế là $x \in A_i$ nhưng lại gán cho $x \in A_j$, $j \neq i$.

Trường hợp 2: $x \in A_j$ nhưng ta lại gán cho $x \in A_i$, $i \neq j$.

Trường hợp 1 xảy ra thì ta nói đã mắc sai lầm loại 1, trường hợp 2 xảy ra thì ta đã mắc sai lầm loại 2. Xác suất mắc sai lầm loại 1 ta ký hiệu là α $(0 \leq \alpha \leq 1)$ và xác suất mắc phải sai lầm loại 2 được ký hiệu là β $(0 \leq \beta \leq 1)$. α là xác suất bác bỏ giả thiết đúng còn β là xác suất chấp nhận giả thiết sai. Dù với thuật toán phân lớp nào cũng không thể triệt tiêu được cả hai loại sai lầm nêu trên. Trong thực tế người ta muốn cố định xác suất sai lầm loại 1, α và xây dựng thuật toán làm cực tiểu hóa sai lầm loại 2, β. Như vậy một thuật toán được cho là tối ưu là thuật toán làm cho tổn thất trung bình của cả hai sai lầm là bé nhất có thể. Bổ đề sau đây nhằm giải quyết bài toán đặt ra:

Trước hết ta ký hiệu z_{ij} là tổn thất khi đối tượng x thực tế là $x \in A_i$ nhưng ta lại quyết định $x \in A_j$, $j \neq i$. Rõ ràng rằng $z_{ii} = 0 \ \forall \ i = 1, 2, \ldots, k$ (k là số lớp). Trái lại, $z_{ij} > 0$ với $i \neq j$.

Nếu đối tượng $x \in A_i$ thì tổn thất trung bình có điều kiện với $x \in A_i$ là:

$$L_i = \sum_{j=1}^{k} z_{ij} \int_{A_j} f_i(x) d\mu(x) \qquad (3.1)$$

Trong đó $\{ f_i(x) \}_{i=\overline{1,k}}$ là k hàm mật độ xác suất của họ phân bố chuẩn $N(\mu_i, \nu_i)$ với $i = 1, 2, \ldots, k$. (Ở đây μ là độ đo σ- hữu hạn trên không gian các tập con của Ω).

Tiếp theo, ta ký hiệu π_i là xác suất để đối tượng $x \in A_i$, tức là $\pi_i = P\{x \in A_i\}$ và giả thiết $\pi_i > 0$, i = 1, 2,…, k.

Do đó giá trị trung bình không điều kiện của tổn thất khi phân lớp $\Omega = \bigcup_{i=1}^{k} A_i$ như sau:

$$L = \sum_{i=1}^{k} \pi_i L_i \qquad (3.2)$$

Đặt $q_j(x) = \sum_{i=1}^{k} \pi_i z_{ij} f_i(x)$, $j = 1, 2, \ldots, k.$ (3.3)

Từ (3.1), (3.2) và (3.3) suy ra rằng:

$$L = \sum_{j=1}^{k} \int_{A_j} q_j(x) d\mu(x) \equiv L(A_1, A_2, \ldots, A_k) \quad (3.4)$$

Từ đó, bài toán đặt ra là: Hãy xây dựng một phân hoạch $A_1^*, A_2^*, \ldots, A_k^*$ sao cho cực tiểu hóa giá trị L:

$L^* = L(A_1^*, A_2^*, \ldots, A_k^*)$, tức là $L^* \le L$.

Ta có bổ đề sau đây:

Bổ đề 1: Giả sử $A_1^*, A_2^*, \ldots, A_k^*$ là một phân hoạch trên tập Ω thỏa mãn điều kiện: $[x \in A_i^*] \Rightarrow [q_i(x) \le q_j(x), j = 1, 2, \ldots, k]$. Khi đó, $L^* = L(A_1^*, A_2^*, \ldots, A_k^*) \le L = L(A_1, A_2, \ldots, A_k)$ đối với mọi phân hoạch $A_1, A_2, \ldots, A_k$ tùy ý trên Ω.

Chứng minh

Thật vậy, từ giả thiết trên ta có:

$$L = L(A_1, A_2, \ldots, A_k) = \sum_{j=1}^{k} \int_{A_j} q_j(x) d\mu(x) = \sum_{j=1}^{k} \sum_{i=1}^{k} \int_{A_j \cap A_i^*} q_j(x) d\mu(x)$$

$$= \sum_{i=1}^{k} \sum_{j=1}^{k} \int_{A_i^* \cap A_j} q_j(x) d\mu(x) \ge \sum_{i=1}^{k} \sum_{j=1}^{k} \int_{A_i^* \cap A_j} q_i(x) d\mu(x) = \sum_{i=1}^{k} \int_{A_i^*} q_i(x) d\mu(x)$$

$= L(A_1^*, A_2^*, \ldots, A_k^*) = L^*$. Đây là điều phải chứng minh.

Chú ý: Để đơn giản trong thực hành ta giả thiết:

$$z_{ij} = \begin{cases} 0 & \text{nếu } i=j \\ 1 & \text{nếu } i \ne j \end{cases} \quad (3.5)$$

Và đặt:

$$c(x) = \sum_{i=1}^{k} \pi_i f_i(x), \quad (3.6)$$

Từ (3.3), (3.5) và (3.6) ta suy ra:

$$q_j(x) = c(x) - \pi_j f_j(x) \quad (3.7)$$

Từ đó, $q_t(x) \le q_j(x)\ \forall\ j = 1, 2,\ldots, k$ nếu và chỉ nếu:

$$\pi_t f_t(x) \ge \pi_j f_j(x)\ \forall\ j = 1, 2,\ldots, k \qquad (3.8)$$

Như vậy nếu tồn tại một $t \ne j$ mà

$$\pi_t f_t(x) > \pi_j f_j(x)\ \forall\ j = 1, 2,\ldots, k \qquad (3.8')$$

thì quyết định của ta về việc $x \in A_t$ là tối ưu.

Trường hợp tồn tại $t_1 \ne t_2$, $t_1 \ne j$, $t_2 \ne j, j = 1, 2,\ldots, k$ mà $\pi_{t_1} f_{t_1}(x) \ge \pi_j f_j(x)$ và đồng thời $\pi_{t_2} f_{t_2}(x) \ge \pi_j f_j(x)\ \forall j \ne t_1, t_2$. Khi đó ta sử dụng quy tắc: $x \in A_{t_1}$ nếu $t_1 > t_2$ và $x \in A_{t_2}$ nếu $t_2 > t_1$.

Bây giờ, giả sử cho một tập hữu hạn Ω đã được phân hoạch tối ưu (theo nghĩa nêu trên). Để đơn giản phân hoạch đó được ký hiệu là $A_1, A_2,\ldots, A_k$, $k \ge 2$ và cho trước. Giả sử $f_1, f_2,\ldots, f_k$ là các hàm mật độ xác suất lần lượt trên $A_1, A_2,\ldots, A_k$.

Ta ký hiệu tập hợp $G = \{f_1, f_2, \ldots, f_k\}$ và h là một hàm mật độ xác suất nào đó của đại lượng ngẫu nhiên Y. Vấn đề đặt ra là hãy trả lời câu hỏi: có tồn tại một *i*, $i = 1, 2,\ldots, k$ mà $y \in A_i$ hay không ?

Sau đây là câu trả lời cho câu hỏi trên:

Bổ đề 2: Cho $f_1, f_2,\ldots, f_k$ là *k* hàm mật độ xác suất lần lượt trên $A_1, A_2, \ldots, A_k$. Trong đó $\{A_1, A_2,\ldots, A_k\}$ là phân hoạch như trong Bổ đề 1. Giả sử X là một đại lượng ngẫu nhiên trên Ω với h là một hàm mật độ xác suất của X trên không gian Ω. Khi đó:

1/ Nếu tích phân $\int_\Omega h(x) \log \frac{f_i(x)}{f_j(x)} d\mu(x) > 0$ với mọi $j \ne i$. Khi đó, $h = f_i$ μ - hầu khắp nơi trên Ω, đặc biệt là trên A_i.

2/ Nếu tồn tại một $j \ne i$ mà $\int_\Omega h(x) \log \frac{f_i(x)}{f_j(x)} d\mu(x) < 0$. Khi đó, $h \ne f_i$.

3/ Nếu $\int_\Omega h(x) \log \frac{f_i(x)}{f_j(x)} d\mu(x) = 0$. Khi đó, không có câu trả lời.

4/ Nếu $\int_{\Omega} h(x)\log\frac{f_i(x)}{f_j(x)}d\mu(x) < 0$ với mọi j $\neq$ i. Khi đó, có tồn tại một $i_0 \neq$ i mà h = f_{i_0} trên Ω trong đó f_{i_0} được xác định như sau:

$$\int_{\Omega} h(x)\log\frac{f_{i_0}(x)}{f_i(x)}d\mu(x) = \max_{j\neq i}\int_{\Omega} h(x)\log\frac{f_j(x)}{f_i(x)}d\mu(x)$$

Chứng minh:

Để chứng minh Bổ đề 2, ta sử dụng Bổ đề 3 với nội dung như sau:

Bổ đề 3: Giả sử f và g là hai làm số thực, không âm và khả tích đối với độ đo μ nào đó trên miền Ω và sao cho thỏa mãn điều kiện:

Tích phân $\int_{\Omega}(f-g)d\mu(x) \geq 0$ (3.9)

Khi đó tích phân $\int_{\Omega} f\log\frac{f}{g}d\mu(x) \geq 0$ (3.10)

và nó bằng 0 khi và chỉ khi f = g μ - hầu khắp nơi trên Ω.

Chứng minh:

Chứng minh Bổ đề 3 cho trường hợp f và g là những hàm rời rạc.

Mệnh đề 1: Cho hai chuỗi số thực không âm và hội tụ: $\sum a_i$, $\sum b_i$ với a_i, b_i ≥ 0 sao cho $(\sum a_i - \sum b_i) \geq 0$. Khi đó $\sum a_i \log\frac{a_i}{b_i} \geq 0$. (3.11)

Bất đẳng thức (3.11) chỉ bằng 0 khi và chỉ khi $a_i = b_i$ với mọi i = 1, 2, 3,…

Chứng minh

Bất đẳng thức (3.11) tương đương với bất đẳng thức (3.12) sau đây:

$$\sum_i a_i \log\frac{b_i}{a_i} \leq 0 \quad (3.12)$$

Ta sẽ chứng minh (3.12) như sau:

Trước hết, ta xét hàm số f(x) = ln$x$ (logarit nêpe) ($\log_a x = \log_e x = \ln x$). Bây giờ ta khai triển hàm f(x) trong lân cận V(1) = (1-ε, 1+ε).

Ta có: ln$x$ = ln(x-1+1)=ln[(x-1)+1] = (x-1)-(x-1)^2($2\xi^2$)$^{-1}$, trong đó $\xi \in (1, x)$.

Vì vậy, $\sum_i a_i \log \frac{b_i}{a_i} = \sum_i a_i[(\frac{b_i}{a_i} - 1) - (\frac{b_i}{a_i} - 1)^2 (2\xi_i^2)]$ = $(\sum b_i - \sum a_i)$ - $\sum_i a_i (\frac{b_i}{a_i} - 1)^2 (2\xi_i^2)] \le 0$ vì $\sum b_i \le \sum a_i$. Đây là điều phải chứng minh.

Bây giờ ta chứng minh Bổ đề 2. Ta ký hiệu tập hợp G = $\{f_1, f_2, \ldots, f_k\}$ và h(x) là hàm mật độ xác suất của đại lượng ngẫu nhiên X trên Ω. Ta giả thiết h$\in$G.

1/ Giả sử tích phân $\int_\Omega h(x) \log \frac{f_i(x)}{f_j(x)} d\mu(x) > 0$, ta cần chứng minh rằng h = f_i μ-hầu khắp nơi trên Ω, đặc biệt là A_i. Thật vậy, giả sử trái lại rằng h $\neq$ f_i, tức là có tồn tại một l để h = f_l. Từ đó và từ giả thiết: $\int_\Omega h(x) \ln \frac{f_i(x)}{f_j(x)} d\mu(x) > 0$ với mọi $j \neq i$, j = 1, 2, …, k. Ta suy ra: $\int_\Omega f_l(x) \ln \frac{f_i(x)}{f_j(x)} d\mu(x) > 0$, vì bất đẳng thức đó đúng cho mọi j nên nó cũng đúng cho j = l, tức là $\int_\Omega f_l(x) \ln \frac{f_i(x)}{f_l(x)} d\mu(x) > 0$, hay $\int_\Omega f_l(x) \ln \frac{f_l(x)}{f_i((x)} d\mu(x) < 0$. Điều này trái với kết quả của Bổ đề 3, vậy h = f_i và Bổ đề được chứng minh.

2/ Hiển nhiên (suy ra từ 1).

3/ Trường hợp $\int_\Omega h(x) \log \frac{f_i(x)}{f_j(x)} d\mu(x) = 0$ thì theo Bổ đề 3 $f_i = f_j$ μ-hầu khắp nơi trên Ω, nên chúng ta không có cơ sở để kết luận h = f_i hay h = f_j.

4/ Thật vậy, do $\int_\Omega h(x) \log \frac{f_i(x)}{f_j(x)} d\mu(x) < 0$ tức là $-\int_\Omega h(x) \log \frac{f_j(x)}{f_i(x)} d\mu(x) < 0$. Điều này có nghĩa là $\int_\Omega h(x) \log \frac{f_j(x)}{f_i(x)} d\mu(x) > 0$ với mọi j$\neq$ i. Do đó có f_{i_0} để $\int_\Omega h(x) \log \frac{f_{i_0}(x)}{f_i(x)} d\mu(x) = \max_{j \neq i} \int_\Omega h(x) \log \frac{f_j(x)}{f_i(x)} d\mu(x) > 0$.

Lấy h = f_{i_0} trên miền Ω. Áp dụng kết quả ở 1/ của Bổ đề này, ta được điều phải chứng minh.

Như vậy, luận án đã trình bày kết quả của việc giải bài toán phân lớp có giám sát (supervised classification) và với số lớp k đã cho trước để phân hoạch được tập Ω thành k lớp: $A_1, A_2,\ldots, A_k$ với $A_i \neq \varnothing$, $i = 1, 2,\ldots, k$ và xác định được $y = x$ với $x \in A_i$. Áp dụng bài toán phân lớp có giám sát, đã phân lớp được đối tượng y nằm trong một tập con A_i của tập hợp các đối tượng Ω. Trường hợp này đơn giản hơn bài toán phân lớp không có giám sát (non-supervised classification) với số lớp k chưa biết nhưng nó phục vụ yêu cầu của bài toán định vị đối tượng đã đặt ra.

3.3.2.3. Phương pháp xác định đối tượng

Sau khi phân lớp được đối tượng, việc tiếp theo cần xác định (tức nhận biết) được đối tượng đó tương ứng với một đầu cuối thiết bị di động (MS/UE) nào đang hoạt động để đưa vào bài toán định vị.

a. Bài toán đặt ra

Giả sử có một đối tượng, liên quan đến một đầu cuối di động MS/UE. Theo số liệu được cung cấp hoặc kiểm tra được, biết rằng MS/UE đó nằm trong một vùng A. Vùng A hiện có một số Cell di động đang hoạt động. Hãy xác định Cell nào đó có khả năng cung cấp dịch vụ tốt nhất cho MS/UE đó, tức là khả năng cao nhất là đối tượng đang nằm trong vùng Cell đó.

b. Giải quyết bài toán

Có một thuật toán xác định được các vùng không gian đặc trưng không chồng lấn lên nhau. Và khi đó, ta chỉ cần phân lớp các Cell là xác định được MS/UE thuộc Cell nào. Tuy nhiên, trong kỹ thuật di động, các vùng phủ Cell tức không gian của Cell là chồng lấn lên nhau. Do vậy, mô hình giải thuật nhận biết được MS/UE đó nằm trong Cell nào cần tận dụng kỹ thuật phân tích tín hiệu điều khiển chuyển vùng bằng bài toán phân lớp không có giám sát (un-supervision) tức là không cho trước các thông tin về đối tượng phân lớp.

Mô hình thực hiện như sau:

- Mỗi một MS/UE$^{(i)}$ (thuê bao thứ *i*) được đặc trưng bởi véc tơ (gọi là véc tơ đặc trưng – characteristic vector) $\mathbf{V}^{i)} = [V_1^{(i)}, V_2^{(i)},\ldots, V_n^{(i)}]$ trong không gian véc tơ *n*

chiều. Trong đó $V_j^{(i)}$ biểu diễn cường độ tín hiệu thu được từ trạm phát BTS/eNB thứ *j* của thuê bao thứ *i*, *n* biểu diễn số trạm phát BTS/eNB có thể cung cấp dịch vụ cho MS/UE$^{(i)}$.

Quá trình chuyển vùng tương đương với việc xác định vị trí của véc tơ đặc trưng trong miền (vùng) định trước. Điều này được thực hiện thông qua véc tơ thành phần $V_j^{(i)}$ gán cho MS/UE$^{(i)}$. MS/UE$^{(i)}$ được quyết định bởi trạm phát thứ *j* (*j = 1, 2, ..., n*) nếu: $V_j^{(i)} = \max_{1 \le l \le n} \{V_l^{(i)}\}$

Để đi vào chi tiết và làm rõ hơn vấn đề này, ta đi sâu nghiên cứu và đề xuất giải pháp giải bài toán phân lớp không có giám sát dựa trên khoảng cách Hamming.

Bài toán tổng quát:

Cho một tập hợp hữu hạn các đối tượng tùy ý được gọi là tập tổng quát (Universe) và đươc ký hiệu là Ω, mỗi phần tử của Ω được gọi là một đối tượng (object). Mỗi một phần tử thuộc Ω đều tương ứng 1-1 với một phần tử $x \in G \subset R^n$ (không gian thực *n* chiều). Như vậy việc phân lớp trên không gian Ω tương đương với việc phân lớp trên tập hữu hạn *G*. Mỗi $x \in G$ được coi như một véc tơ *n* chiều. Để đơn giản nhưng không mất tính tổng quát, chúng ta giả thiết rằng $G = \{0,1\}^n$. Như vậy mỗi $x \in G$ là một véc tơ nhị phân *n* thành phần và được ký hiệu là: $x = (x_1, x_2, \ldots, x_n)$ với $x_i \in \{0, 1\}$, $i = 1, 2, 3, \ldots, n$.

Từ đó bài toán phân lớp được đặt ra như sau:

Hãy phân hoạch (partition) tập *G* thành *k* tập con khác rỗng $G_1, G_2, \ldots, G_k$ ($k \ge 2$) sao cho thỏa mãn các yêu cầu sau đây:

i/ $G_i \cap G_j = \varnothing$, với mọi cặp (i, j), $i \ne j$, $i, j = 1, 2, \ldots, k$.

ii/ $\bigcup_{i=1}^{k} G_i = G$

iii/ Sai số trung bình trong quá trình phân hoạch là bé nhất có thể.

Một số khái niệm cơ bản:

Việc xây dựng thuật toán phân lớp thỏa mãn 2 yêu cầu (i) và (ii) là rất dễ dàng. Tuy nhiên việc phân lớp thỏa mãn yêu cầu (iii) là một khó khăn. Hơn nữa đây lại là bài toán phân lớp không có giám sát, tức là chưa cho trước các thông tin tiên nghiệm (prior information) mà *G* chỉ là tập hữu hạn các dữ liệu (dạng véc tơ). Do đó, để giải bài toán này, ta cần đưa ra các khái niệm: thế nào là khoảng cách giữa 2 véc tơ (nhị phân), thế nào là sự gần gũi giữa 2 tập hợp (tức độ đo sự khác nhau (giống nhau) giữa 2 tập hợp)? Ta có các định nghĩa sau:

Định nghĩa 1: Cho *X* là một tập hợp khác rỗng tùy ý, khi đó khoảng cách giữa hai phần tử $x, y \in X$ là một ánh xạ:

$d: X \times X \to R=(-\infty, +\infty)$

thỏa mãn 3 tiên đề sau đây:

Tiên đề 1: $d(x,y) \geq 0$, đối với mọi $x, y \in X$

Tiên đề 2: $d(x,y) = d(y,x)$

Tiên đề 3: $d(x,y) \leq d(x,z) + d(z,y)$, đối với mọi $x, y, z \in X$.

Có một số độ đo khoảng cách đã được định nghĩa. Trong phần này, luận án đưa ra một độ đo khoảng cách được gọi là khoảng cách Hamming như sau:

Lấy $X = G$ và xác định: $d(x,y)=\frac{1}{n}\sum_{i=1}^{n}(x_i \oplus y_i)$, trong đó $x=(x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$, với $x_i, y_i \in \{0, 1\}$, $i = 1, 2, 3, \ldots, n$.

Định nghĩa khoảng cách như vậy rõ ràng thỏa mãn 2 tiên đề 1 và 2. Ta chỉ cần chứng minh nó cũng thỏa mãn với cả tiên đề 3.

Thật vậy, giả sử cho $x, y, z \in G$, ta có theo định nghĩa:

$$d(x,y)=\frac{1}{n}\sum_{i=1}^{n}(x_i \oplus y_i)$$

$$=\frac{1}{n}\sum_{i=1}^{n}[(x_i \oplus y_i)+(z_i \oplus z_i)]$$

$$=\frac{1}{n}\sum_{i=1}^{n}[(x_i \oplus z_i)+(z_i \oplus y_i)]$$

$$=\frac{1}{n}\sum_{i=1}^{n}\left|(x_i \oplus z_i)+(z_i \oplus y_i)\right|$$ (vì $|a|=a$ nếu a không âm).

Từ đó ta có: $d(x,y) \le \frac{1}{n}\sum_{i=1}^{n}|x_i \oplus z_i| + \frac{1}{n}\sum_{i=1}^{n}|z_i \oplus y_i|$

$= \frac{1}{n}\sum_{i=1}^{n}(x_i \oplus z_i) + \frac{1}{n}\sum_{i=1}^{n}(z_i \oplus y_i) = d(x,z) + d(z,y).$

Định nghĩa 2: Cho trước k tập hợp con hữu hạn, khác rỗng $G_1, G_2, \ldots, G_k$ ($k \ge 2$). Ta định nghĩa khoảng cách giữa 2 tập hợp G_i, G_j = là: $\rho(G_i, G_j) = \frac{1}{n_i n_j}\sum_{x \in G_i}\sum_{y \in G_j} d(x,y)$, được gọi là khoảng cách trung bình giữa 2 tập khác nhau.

Trong đó $n_i = |G_i|$ là số phần tử trong tập hợp G_i, với $i = 1, 2, \ldots, k$. Nếu $i \ne j$ thì $\rho(G_i, G_j)$ được gọi là giá trị ngoài của 2 tập hợp G_i, G_j. Trường hợp $i = j$, thì ta định nghĩa: $\rho(G_i, G_j) = \frac{2}{n_i(n_i - 1)}\sum_{x \in G_i}\sum_{y \in G_i} d(x,y)$ và được gọi là giá trị trong của tập hợp G_i (tức là $\rho(G_i, G_i)$ là khoảng cách trung bình giữa các điểm của tập hợp G_i, với $i = 1, 2, \ldots, k$.

Luận án đề xuất thuật toán giải bài toán phân lớp không có giám sát như sau:

Cho trước $G = \{x^{(1)}, x^{(2)}, \ldots, x^{(m)}\} \subset \{0,1\}^n$. Hãy phân hoạch (partition) tập G thành k tập con sao cho sai số về trung bình là nhỏ nhất.

Thuật toán

Bước 1. Đặt $G_1 = \{x^{(1)}\}$, $G_2 = \{x^{(2)}\}$, …, $G_m = \{x^{(m)}\}$

Bước 2. Tính $\min_{1 \le i \ne j \le m} \rho(G_i, G_j) = \rho(G_{i_0}, G_{j_0})$

Bước 3. Cho $i = 1, 2, \ldots, k$. Đặt $G_i = \{(G_{i_0}, G_{j_0}\}$

Bước 4. $i := i+1$ và tính $\min_{l,m \ne (i_0, j_0)} \rho(G_l, G_m) = \rho(G_{l_0}, G_{m_0}) = G_i$.

Bước 5. Nếu $i \ge k$ thì thuật toán dừng.

Bước 6. Đi đến bước 4.

Như vậy từ tập G, ta đã tách ra làm k tập con rời nhau, mà ta ký hiệu là $G_1, G_2, \ldots G_k$

Như vậy, luận án đã đưa ra một thuật toán phân lớp không có giám sát sao cho sai số của phân lớp là nhỏ nhất mà không phụ thuộc vào việc điều khiển chuyển vùng. Kết quả nghiên cứu đã chỉ ra rằng, để giải bài toán phân lớp không có giám sát, tìm ra MS/UE thuộc Cell (trạm phát nào) đang phục vụ thì phải tính toán các véc tơ đặc trưng của nó thông qua tính khoảng cách Hamming. Trên cơ sở dữ liệu đã được phân lớp, thuật toán định vị đối tượng liên quan đến việc điều khiển chuyển vùng được áp dụng để định vị MS/UE đó, tức đối tượng đó.

[C2, J1; 18-22].

3.3.3. Lựa chọn kỹ thuật phân lớp xác định đối tượng định vị

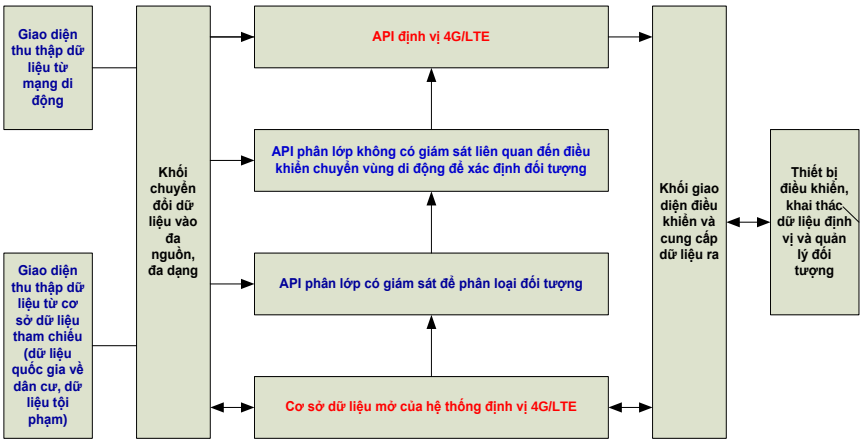
Căn cứ vào kết quả các nghiên cứu về phân lớp có giám sát và phân lớp không có giám sát ở trên, luận án đề xuất giải pháp kỹ thuật "phân lớp hỗn hợp" để xác định một đối tượng định vị là:

- Sử dụng thuật toán phân lớp có giám sát để phân loại đối tượng.

- Sau đó sử dụng thuật toán phân lớp không có giám sát liên quan tới điều khiển chuyển vùng để xác định chính xác tập dữ liệu đặc trưng của đối tượng (trong đó có dữ liệu vùng Cell phục vụ), cung cấp dữ liệu đầu vào của bài toán (nguyên lý kỹ thuật) định vị sẽ được ứng dụng.

Luận án đề xuất mô hình ứng dụng hệ thống xác định đối tượng định vị 4G của CQAN bằng giải pháp kỹ thuật phân lớp hỗn hợp như sau:

3.3.3.1. Sơ đồ cấu trúc hệ thống



Hình 3. 3. Mô hình hệ thống phân lớp, xác định đối tượng định vị

3.3.3.2. Mô tả chức năng hệ thống

Các thuật toán phân lớp đã được nghiên cứu sẽ được lập trình thành 2 giao diện lập trình ứng dụng API để chạy trên nền tảng Trung tâm định vị 4G/LTE. Thuật toán API phân lớp có giám sát sẽ lấy dữ liệu từ nguồn cơ sở dữ liệu mở có sẵn trong trung tâm cùng với dữ liệu cập nhật từ các nguồn tham chiếu của hệ thống. API này sẽ tính toán phân lớp đối tượng ra thuộc lớp nào.

Sau đó, lớp đối tượng sẽ được cung cấp cho API phân lớp không có giám sát liên quan đến điều khiển chuyển vùng di động, cùng với dữ liệu điều khiển chuyển vùng lấy từ nhà mạng, API sẽ tính toán và xác định được đối tượng với tập dữ liệu đặc trưng của nó liên quan đến bài toán định vị và cung cấp cho các API xử lý định vị. Các dữ liệu đặc trưng của đối tượng là cơ sở để hệ thống xác định được nguyên lý kỹ thuật, thuật toán tối ưu sẽ được sử dụng để tính toán vị trí thiết bị di động.

3.4. Bảo mật chuyển giao kết quả định vị

Kết quả định vị là một loại số liệu, dữ liệu quan trọng mà CQAN cần chuyển giao đến các địa chỉ khác nhau. Vì tính chất bí mật của nó cùng với thực tiễn khả năng bảo mật của các đường truyền dữ liệu, nội dung sau đây sẽ trình bày về phương pháp bảo mật chuyển giao kết quả định vị.

3.4.1. Bảo mật chuyển giao kết quả định vị sử dụng bài toán chia sẻ mảnh bí mật qua ảnh

Hiện nay, bài toán chia sẻ bí mật (Secret Share) đang có nhiều ứng dụng trong thực tiễn. Có những yêu cầu bảo mật mà phải đảm bảo rằng chỉ chia sẻ cho một số người nhận nhất định và chỉ khi những người nhận đó cùng đồng thuận thì mới có thể mở được bí mật đó. Mỗi thành viên giữ một phần (mảnh) của chìa khóa sao cho chỉ có thể tất cả thành viên cùng đồng thuận thì mới có thể sử dụng được chìa khóa đó. Trong trường hợp chuyển giao kết quả định vị cho một nhóm trinh sát hành động, mà yêu cầu mỗi người chỉ nắm được một phần kết quả, chỉ khi tất cả các thành viên trong nhóm trinh sát đồng thuận mới có được kết quả toàn bộ.

Trong phần này, luận án trình bày một phương pháp phân phối các mảnh bí mật đó bằng một thuật toán đơn giản nhưng an toàn và khả thi trong thực hành, sử dụng thuật toán chia sẻ bí mật phân mảnh để nhúng thông tin mật vào chính ảnh của thành viên nhóm, như thuật toán đề xuất dưới đây.

3.4.1.1. Mô hình hệ thống

- Đặt bài toán

Giả sử có n thành viên A_1, A_2, ., A_n phối hợp cùng nhau sẽ nắm giữ một bí mật $A_0 \in E_p^*$ nào đó. Trong đó, p là số nguyên tố đủ lớn sao cho $[\sqrt{p}\,]>n$. Bài toán đặt ra là mỗi thành viên A_j chỉ nắm được một phần bí mật A_0 và một tập hợp bất kỳ các thành viên có lực lượng bé hơn n đều không thể khôi phục được bí mật A_0. Chỉ khi đúng cả n thành viên kết hợp lại với nhau mới khôi phục được giá trị bí mật A_0.

- Giải bài toán

Lược đồ giải bài toán như sau:

Bước 1. Người được ủy quyền (Trung tâm) chọn số nguyên tố p đủ lớn sao cho $[\sqrt{p}\,]>n$ (ký hiệu $[\sqrt{p}\,]$ là phần nguyên của $\sqrt{p}$).

Bước 2. Người được ủy quyền chọn $2n$-1 phần tử ngẫu nhiên trong trường hữu hạn $Z_p = \{0,1,2,...,p\text{-}1\}$, được ký hiệu là $a_1, a_2, \ldots, a_{n-1}$; $v_0, v_1, v_2, \ldots, v_{n-1}$. Trong đó tất cả $v_j \neq 0$ và ước chung lớn nhất (GCD – Greatest Common Divisor) của v_i, v_j bằng 1, tức là $GCD(v_i,v_j) = 1$, với $i \neq j$.

Bước 3. Người được ủy quyền xác định một đa thức

$$f(x)= a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1x^1 + A_0 \,(mod\ p)$$

Bước 4. Mỗi A_j nhận được từ người được ủy quyền cặp $(v_j,f(v_j)) \in E_p^* \times E_p^*$, j = 0, 1, …, n-1.

Để khôi phục lại bí mât A_0, tất cả n thành viên hợp lại mới khôi phục được A_0 bằng đa thức

$$g(x)= \sum_{0\le j<n} f(v_j) \prod_{0\le i\le n, i\neq j} (v_j - v_i)^{-1}(x - v_i)\ (mod\ p)$$

- Tính đúng đắn của lược đồ

Cơ sở của lược đồ chia sẻ bí mật là định lý sau:

Định lý 1: *n* thành viên của lược đồ chia sẻ bí mật ở trên có thể tính toán một cách có hiệu quả $g(0)=A_0$.

Chứng minh: Dễ thấy rằng phép nội suy Lagrange của hàm f là một đa thức có bậc nhỏ hơn n và g thỏa mãn:

$$g(v_j)=f(v_j) \text{ với } 0 \leqslant j < n.$$

Do đó, f - g là một đa thức trên Z_p có cấp nhỏ hơn *n*, nhưng nó lại có ít nhất là *n* nghiệm phân biệt, được đánh số *r* với $f(r) - g(r) = 0$. Điều đó chứng tỏ rằng $f(a) = g(a)$ với mỗi $a \in Z_p$.

Đặc biệt ta có $A_0 = f(0) = g(0)$ đó chính là giá trị bí mật A_0.

Theo lược đồ thì các giá trị $(v_j,f(v_j))$ với $j = 0, 1, n-1$ được chuyển cho các thành viên A_j trên mạng công cộng. Trong phần này không nói rõ là người có thẩm quyền chuyển các $(v_j,f(v_j))$ đến thành viên A_j bằng cách nào. Nếu chuyển các mảnh bí mật này trên kênh công cộng mà không có sự bảo vệ tốt thì các mảnh này không đảm bảo an toàn. Thật vậy, nếu người được ủy quyền chuyển $(v_j,f(v_j))$ cho A_j một cách công khai thì có thể một người khác được ký hiệu là A'_j có thể bắt được mảnh bí mật đó trước khi nó đến tay người nhận đích thực A_j với $j = 0, 1, n-1$. Như vậy các thành viên A'_j với $j = 0, 1, n-1$ có được trong tay *n* mảnh bí mật và do đó họ khôi phục lại được bí mật A_0. Vì vậy việc chuyển các mảnh bí mật $(v_j,f(v_j))$ phải thực hiện một cách bí mật. Nhưng nếu các $(v_j,f(v_j))$ được mã hóa bằng mật mã khóa đối xứng thì vấn đề trao đổi khóa trở nên rất phức tạp nếu *n* lớn. Còn nếu sử dụng mã khóa công khai chẳng hạn sử dụng mã RSA thì phải sinh cặp n các số nguyên tố khác nhau và đủ lớn (mỗi số nguyên tố phải có độ lớn > 512 bit) và do đó việc quản lý các tham số cho hệ mật đó là một vấn đề. Để giải quyết vấn đề trao đổi các mảnh bí mật $(v_j,f(v_j))$ đã được trình bày ở trên, luận án đề xuất một phương pháp được trình bày dưới đây.

3.4.1.2. Thuật toán được đề xuất

Luận án đề xuất một phương pháp trao đổi các mảnh bí mật (v_j,f(v_j)): **Giấu (v_j,f(v_j)) vào ảnh của thực thể A_j (j=0, 1, …., n-1).** Từ nay, ta gọi (v_j,f(v_j)) là "bí mật" cho đơn giản.

Giả sử P(x) là một đa thức nguyên thủy cấp 5 trong trường GF(2), P(x) = x^5 + x^2 + 1. Đa thức này có 2^5 - 1 nghiệm mở rộng trong trường GF(2). Ta biết rằng ([.]), tập hợp tất cả các nghiệm mở rộng đó cùng với vector 0 = 00000, tạo thành một không gian vector có số chiều là 5. Ta ký hiệu không gian vector đó là V^5. Như vậy trong V^5 có tồn tại một cơ sở trực chuẩn là S = {s_1, s_2, s_3, s_4, s_5} = {(10000), (01000), (00100), (00010), (00001)}.

Ta ký hiệu α là một nghiệm của đa thức P(x), nghĩa là P(α) = $\alpha^5 + \alpha^2 + 1 = 0$. Từ đó ta suy ra $\alpha^5 = \alpha^2 + 1$. Ta có:

$\alpha^6 = \alpha.\alpha^5 = \alpha^3 + \alpha$, $\alpha^7 = \alpha.\alpha^6 = \alpha^4 + \alpha^2$, $\alpha^8 = \alpha.\alpha^7 = \alpha^5 + \alpha^3 = \alpha^3 + \alpha^2 + 1$

Cứ như vậy lần lượt ta có:

$\alpha^9 = \alpha^4 + \alpha^3 + \alpha$, $\alpha^{10} = \alpha^4 + 1$, $\alpha^{11} = \alpha^2 + \alpha + 1$, $\alpha^{12} = \alpha^3 + \alpha^2 + \alpha$, $\alpha^{13} = \alpha^4 + \alpha^3 + \alpha^2$

$\alpha^{14} = \alpha^4 + \alpha^3 + \alpha^2 + 1$, $\alpha^{15} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$, $\alpha^{16} = \alpha^4 + \alpha^3 + \alpha + 1$,

$\alpha^{17} = \alpha^4 + \alpha + 1$, $\alpha^{18} = \alpha + 1$, $\alpha^{19} = \alpha^2 + \alpha$, $\alpha^{20} = \alpha^3 + \alpha^2$, $\alpha^{21} = \alpha^4 + \alpha^3$,

$\alpha^{22} = \alpha^4 + \alpha^2 + 1$, $\alpha^{23} = \alpha^3 + \alpha^2 + \alpha + 1$, $\alpha^{24} = \alpha^4 + \alpha^3 + \alpha^2 + \alpha$, $\alpha^{25} = \alpha^4 + \alpha^3 + 1$,

$\alpha^{26} = \alpha^4 + \alpha^2 + \alpha + 1$, $\alpha^{27} = \alpha^3 + \alpha + 1$, $\alpha^{28} = \alpha^4 + \alpha^2 + \alpha$, $\alpha^{29} = \alpha^3 + 1$, $\alpha^{30} = \alpha^4 + \alpha$

và $\alpha^{31} = \alpha^5 + \alpha^2 = \alpha^0 \equiv (10000)$.

Ta đặt $\alpha = \alpha^0 = (10000)$, ta nhận được bảng sau đây (ký hiệu bảng này là ma trận **A**, **A** = $[(a_{ij})]^T (5\times 31)$, trong đó $a_{ij} \in$ GF(2) i = 1, 2, …, 5; j = 1, 2, …., 31).

$\mathbf{A^T}$ =

$$\begin{bmatrix} 1&0&0&0&0&1&0&0&1&0&1&1&0&0&1&1&1&1&1&0&0&0&1&1&0&1&1&1&0&1&0 \\ 0&1&0&0&0&0&1&0&0&1&0&1&1&0&0&1&1&1&1&1&0&0&0&1&1&0&1&1&1&0&1 \\ 0&0&1&0&0&1&0&1&1&0&0&1&1&1&1&1&0&0&0&1&1&0&1&1&1&0&1&0&1&0&0 \\ 0&0&0&1&0&0&1&0&1&1&0&0&1&1&1&1&1&0&0&0&1&1&0&1&1&0&0&1&0&1&0 \\ 0&0&0&0&1&0&0&1&0&1&1&0&0&1&1&1&1&1&0&0&0&1&1&0&1&1&1&0&1&0&1 \end{bmatrix}$$

Giả sử muốn giấu bí mật (v_j,f(v_j)) và chuyển trên kênh công khai cho thành viên A_j, ta thực hiện như sau:

- Thuật toán giấu

Bước 1. Đổi cặp (v_j,f(v_j)) sang dãy nhị phân.

Bước 2. Chia dãy nhị phân trên thành các block 5 bit một theo thứ tự từ phải sang trái, nếu còn thiếu thì thêm một số bit 0 ở đầu block cho đủ khối 5 bit.

Bước 3. Giả sử $\mathbf{B_1}$, $\mathbf{B_2}$, …, $\mathbf{B_n}$ là các block nhị phân đã được chia ở bước 2.

Bước 4. Trích chọn các LSB (Least Significant Bit) của các pixel của ảnh I, bắt đầu từ một khởi điểm quy định trước giữa trung tâm với A_j cho đến pixel thứ 31n (trong đó n là số block được xác định ở bước 3) và tạo lên n khối (block), mỗi block gồm 31 bit LSB mà ta ký hiệu là $\mathbf{L_1}$, $\mathbf{L_2}$,…, $\mathbf{L_n}$ (mỗi $\mathbf{L_i}$ gồm 31 bit, i = 1, 2, …., n).

Bước 5. Với i = 1, 2, …., n. Tính $\mathbf{C_i^T = B_i^T \oplus A^T L_i^T}$.

Bước 6. Tìm xem trong ma trận $\mathbf{A^T}$ có cột nào trùng với $\mathbf{C_i^T}$ hay không.

Nếu không có cột nào của $\mathbf{A^T}$ trùng với $\mathbf{C_i^T}$ thì bỏ qua.

Nếu tồn tại ở cột thứ m của ma trận $\mathbf{A^T}$ trùng với $\mathbf{C_i^T}$ thì tại vị trí thứ m của block $\mathbf{L_i}$ sẽ thực hiện việc đảo bit (1 thành 0 và ngược lại).

Bước 7. Đặt $i = i + 1$ và quay lại bước 5, cứ tiếp tục cho đến khi $i = n$.

Như vậy sau bước 7 ta nhận được $\mathbf{C_1}$, $\mathbf{C_2}$, …, $\mathbf{C_n}$,

Bước 8. Trong ảnh của A_j các $\mathbf{L_1}$, $\mathbf{L_2}$,…, $\mathbf{L_n}$ được thay thế bởi $\mathbf{C_1}$, $\mathbf{C_2}$, …, $\mathbf{C_n}$, ta nhận được ảnh S_j.

Bước 9. Chuyển S_j cho A_j.

Bước 10. Cho $j = j + 1$ và trở lại bước 1 như đã trình bày ở trên.

- Thuật toán trích chọn

Sau khi nhận được ảnh S_j, A_j tiến hành trích chọn một mảnh bí mật $(v_j,f(v_j))$ như sau:

Bước 1. Bắt đầu từ vị trí khởi điểm đã được trung tâm quy ước trước với từng A_j; j=0, 1, .., n-1 (hay j= 1, 2, .., n) A_j sẽ trích chọn ra 31n bít LSB của các pixel của ảnh S_j và tạo thành n block có độ dài bằng nhau và bằng 31 và được ký hiệu là $\mathbf{C_1}$, $\mathbf{C_2}$, …, $\mathbf{C_n}$.

Bước 2. Với i = 1, 2, …., n. Tính $\mathbf{B_i^T = A_i^T C_i^T}$ ta nhận được $\mathbf{B_1}$, $\mathbf{B_2}$, …, $\mathbf{B_n}$,

Bước 3. Chuyển đổi dãy nhị phân thành số thập phân (nếu cần) ta nhận được $(v_j,f(v_j))$.

Chú ý: Trong bước 2 của thuật toán giấu, việc chia dãy nhị phân được thực hiện từ phải sang trái và nếu block cuối cùng (tức là block đầu tiên tính từ bên trái) chưa đủ 5 bit thì thêm các bit 0 cho đủ. Còn v_j cách $f(v_j)$ bởi vector 00000.

3.4.1.3. Kết quả thử nghiệm

Trong phần này, luận án trình bày kết quả giải bài toán chia sẻ bí mật qua một trường hợp cụ thể sau đây:

Cho số nguyên tố p=1999

Cho n=3, ta có 3 thành viên A_1, A_2, A_3

Người được ủy quyền chọn ngẫu nhiên, chẳng hạn:

a_1= 334, a_2=223; v_0=626, v_1=674, v_2=93. Cho bí mật A_0=472.

Sau đó người được ủy quyền tính:

$f(v_0)$=1724

$f(v_1)$=1925

$f(v_2)$=1241

Người ủy quyền chuyển $(v_j,f(v_j))$ cho A_j, j=0,1, 2.

Hay cặp $(v_0,f(v_0))$ = (626, 1724) cho A_1

$(v_1,f(v_2))$ = (674, 1925) cho A_2

$(v_2,f(v_2))$ = (93, 1241) cho A_3

Rõ ràng là 2 trong 3 thành viên không thể khôi phục được bí mật, mà cả 3 thành viên trong nhóm mới khôi phục được A_0 như sau:

$$A_0 = \sum_{0 \le j < 3} f(v_j) b_j \ mod\ 1999 \qquad (*)$$

Trong đó: $b_j = \prod_{0 \le i < 3} v_i (v_i - v_j)^{-1} \ mod\ 1999$

Từ (*) ta có:

A_1 tính được: b_0 =1847

A_2 tính được: b_1 =793

A_3 tính được: b_2 =1359

Từ cả 3 thành viên, áp dụng công thức (*), ta tính được: A_0=472 là giá trị bí mật do người ủy quyền chuyển cho. Bí mật này có thể là khóa mã hoặc thông tin mật nào đó.

Tuy nhiên, các phương pháp chia sẻ bí mật hiện nay không trình bày cách thức trao đổi các giá trị bí mật (v_j,f(v_j)) cho các thực thể A_j , j = 0,1,... n-1 như thế nào. Nếu các giá trị này không đảm bảo an toàn thì bài toán chia sẻ bí mật được đưa ra đều vô nghĩa. Mục đích chính của phần này là đề xuất một thuật toán trao đổi các thành phần bí mật (v_j,f(v_j)) cho các thành viên của nhóm tương đối đơn giản bằng cách giấu thông tin mật đó vào chính ảnh của mỗi thành viên. Để trích chọn yêu cầu mỗi thành viên biết trước khởi điểm giấu của thuật toán và độ dài của giá trị (v_j,f(v_j)), j = 0,1,..., n-1. *[C3; 13-17]*.

3.4.2. Bảo mật chuyển giao kết quả định vị sử dụng thuật toán giấu tin mật qua ảnh

Các hệ thống mã hóa hiện nay không đáp ứng được đầy đủ các yêu cầu về bảo mật thông tin trong thực tế khi công nghệ thông tin đang ngày càng phát triển. Chẳng hạn, việc bảo mật hai đầu gửi và nhận trong hệ thống thông tin liên lạc có bảo mật; hoặc các dữ liệu lưu và truyền trên mạng dùng chung cần được chia sẻ nhưng cần được bảo vệ tính riêng tư của tác giả. Một hướng tiếp cận mới đã được nghiên cứu và hiện nay đang phát triển để giải quyết vấn đề này, đó là kỹ thuật giấu tin trong Đa phương tiện, đặc biệt là kỹ thuật giấu tin trong ảnh số và trong âm thanh số.

Trong bài toán định vị đối tượng, cần phải trao đổi dữ liệu đầu vào hoặc kết quả định vị đến, từ nhiều nơi, nhiều người dùng. Do đó, yêu cầu bảo mật chuyển giao kết

quả định vị được đặt ra. Việc bảo mật đường truyền, sẽ được cung cấp bởi các cơ quan chuyên môn theo qui định. Riêng tập dữ liệu đầu vào được thu thập để phục vụ định vị di động và dữ liệu kết quả định vị đầu ra được chuyển giao từ trung tâm đến nơi nhận qua những môi trường không an toàn như Internet hoặc điện thoại di động 4G, luận án đề xuất sử dụng giải pháp bảo mật bằng cách nhúng thông tin vào ảnh kỹ thuật số truyền đi, vừa phải đảm bảo tính nhanh chóng, tức thời của việc chuyển giao. Để đảm bảo an toàn, bí mật cho dữ liệu định vị, thuật toán giấu tin mật qua ảnh phải đạt được được hai tính chất cơ bản là:

- Tính không thể cảm nhận được sự khác biệt giữa ảnh gốc (C) và ảnh sau khi đã giấu tin;

- Lượng thông tin giấu được rất lớn nhưng tỷ lệ tin giấu so với lượng LSB lại rất bé. Ngoài ra thuật toán được đề xuất không dùng đến phương pháp trao đổi khóa, ở đây, khái niệm "khóa" chỉ là những qui ước đơn giản và dễ nhớ.

3.4.2.1. Cơ sở toán học

- Các ký hiệu:

+ GF(p)được ký hiệu là trường Galois có cấp là số nguyên tố p;

+ GF(p)[x] là không gian vector gồm tất cả các đa thức trên trường Galois GF(p).

- Đa thức nguyên thủy

Định nghĩa 1: Một đa thức f(x) cấp m trong trường GF(q) được gọi là đa thức bất khả quy (irreducible polynomial) nếu nó không thể phân tích được thành tích các đa thức có cấp nhỏ hơn m trong trường GF(q).

Ví dụ: f(x) = $x^2 + x + 1$, f(x) = $x^{11} + x^2 + 1$, là những đa thức bất khả quy trên trường GF(2).

Định nghĩa 2: Một đa thức bất khả quy p(x) có cấp m trên trường GF(p) được gọi là đa thức nguyên thủy (primitive polynomial) nếu số nguyên dương nhỏ nhất n mà x^n - 1 chia hết cho p(x) là $n = p^m - 1$.

Ví dụ: Đa thức p(x) = x^3 + x + 1 là đa thức nguyên thủy trên trường GF(2) vì rõ ràng p(x) = x^3+ x + 1 là đa thức bất khả quy và $n = 2^3 - 1 = 7$ là số nguyên dương nhỏ nhất mà x^7 - 1 chia hết cho p(x). (Chú ý: Trong trường GF(2) thì $a + a = a - a =$

0 đối với mọi $a \in GF(2)$ và trong phạm vi luận án, ta chỉ làm việc với trường GF(2)). Một câu hỏi đặt ra là: vậy có bao nhiêu đa thức nguyên thủy cấp m trong trường GF(2)? Ta có định lý sau:

Định lý 1. Có tất cả $Ø(2^m - 1)/m$ đa thức nguyên thủy cấp m trên trường GF(2). Trong đó Ø(.) là hàm Phi - ơle. Ví dụ với $m = 3$, khi đó sẽ có $Ø(3) = 2$. Vậy có 2 đa thức nguyên thủy cấp 3 trong trường GF(2).

Định lý 2. Tập tất cả các nghiệm $\{\alpha_j\}$ của đa thức nguyên thủy p(x) cấp m trong trường GF(2) sẽ có cấp $2^m - 1$.

Bây giờ, giả sử, α là một nghiệm của đa thức nguyên thủy p(x) cấp m, $p(x) = x^m + a_{m-1}x^{m-1} + ... + a_1x + a_0$ trong trường GF(2). Nếu α là một nghiệm của p(x), tức là $p(\alpha) = 0$, thế thì $p(\alpha) = \alpha^m + a_{m-1}\alpha^{m-1} + ... + a_1\alpha + a_0 = 0$.

Từ đó, ta suy ra: $\alpha^m = -a_0 - a_1\alpha - ... - a_{m-1}\alpha^{m-1}$. Các lũy thừa của α có cấp lớn hơn hoặc bằng m có thể được biểu diễn dưới dạng đa thức có cấp nhỏ hơn m. Vì α có cấp $2^m - 1$ nên các lũy thừa khác nhau của α phải có $2^m - 1$ các biểu diễn đa thức phân biệt khác không dưới dạng: $p(\alpha) = b_0 + b_1\alpha + ... + b_{m-1}\alpha^{m-1}$, với $b_i \in GF(2)$, $i = 0,1,2,\ldots, m-1$.

Như vậy, GF(2^m) có thể được coi như là một không gian vector trên trường GF(2).

Tập hợp các vector đó lập thành một không gian vector trên trường GF(2).

Bây giờ chúng ta lấy $m = 64$. Khi đó, không gian vector GF(2^{64}) trên trường GF(2) sẽ gồm tất cả 64 phần tử, mỗi phần tử là một vector độ dài $m = 6$. Để tạo ra một không gian vector như vậy, trước hết chúng ta chọn một đa thức nguyên thủy cấp $m = 6$ trên trường GF(2). Dễ dàng thấy rằng $p(x) = x^6 + x + 1$ là một đa thức nguyên thủy trên trường GF(2). Bằng lý luận như trên, ta nhận được $2^6 - 1$ nghiệm α (trừ phần tử (0,0,0,0,0,0)) là:

Ma trận **H**: Trước hết ta xây dựng một Ma trận **H** = ($h_{.1}$,$h_{.2}$,...,$h_{.63}$), trong đó, $\mathbf{h}_{.j}$ là cột thứ j ($j = 1,2,...,63$) và 6 hàng được thiết lập trước. Cụ thể như sau:

$h_{.1} = (100000)^T$,	$h_{.22} = (110111)^T$	$h_{.43} = (010111)^T$
$h_{.2} = (010000)^T$,	$h_{.23} = (101011)^T$	$h_{.44} = (111011)^T$
$h_{.3} = (001000)^T$,	$h_{.24} = (100101)^T$	$h_{.45} = (101101)^T$
$h_{.4} = (000100)^T$,	$h_{.25} = (100010)^T$	$h_{.46} = (100110)^T$

$h_{.5} = (000010)^T$, $h_{.26} = (010001)^T$ $h_{.47} = (010011)^T$

$h_{.6} = (000001)^T$, $h_{.27} = (111000)^T$ $h_{.48} = (111001)^T$

$h_{.7} = (110000)^T$, $h_{.28} = (011100)^T$ $h_{.49} = (101100)^T$

$h_{.8} = (011000)^T$, $h_{.29} = (001110)^T$ $h_{.50} = (010110)^T$

$h_{.9} = (001100)^T$, $h_{.30} = (000111)^T$ $h_{.51} = (001011)^T$

$h_{.10} = (000110)^T$, $h_{.31} = (110011)^T$ $h_{.52} = (110101)^T$

$h_{.11} = (000011)^T$ $h_{.32} = (101001)^T$ $h_{.53} = (101010)^T$

$h_{.12} = (110001)^T$ $h_{.33} = (100100)^T$ $h_{.54} = (010101)^T$

$h_{.13} = (101000)^T$ $h_{.34} = (010010)^T$ $h_{.55} = (111010)^T$

$h_{.14} = (010100)^T$ $h_{.35} = (001001)^T$ $h_{.56} = (011101)^T$

$h_{.15} = (001010)^T$ $h_{.36} = (110100)^T$ $h_{.57} = (111110)^T$

$h_{.16} = (000101)^T$ $h_{.37} = (011010)^T$ $h_{.58} = (011111)^T$

$h_{.17} = (110010)^T$ $h_{.38} = (001101)^T$ $h_{.59} = (111111)^T$

$h_{.18} = (011001)^T$ $h_{.39} = (110110)^T$ $h_{.60} = (101111)^T$

$h_{.19} = (111100)^T$ $h_{.40} = (011011)^T$ $h_{.61} = (100111)^T$

$h_{.20} = (011110)^T$ $h_{.41} = (111101)^T$ $h_{.62} = (100011)^T$

$h_{.21} = (001111)^T$ $h_{.42} = (101110)^T$ $h_{.63} = (100001)^T$.

Trong đó, $(\mathbf{X})^T$ là chuyển vị của vecto **(X)**.

Trên cơ sở ma trận **H**, chúng ta xây dựng Thuật toán giấu tin mật sau đây.

3.4.2.2. Thuật toán giấu tin mật

- Thuật toán giấu tin:

Input: Bản thông báo M = (m_1, m_2,..., m_n), $m_i \epsilon$ { a,b,c,...,z}; ảnh BitMap C, khởi điểm (điểm bắt đầu đặt bít dữ liệu vào ảnh C), và độ dài mẫu ZIP(M) = X = (x_1, x_2,..., x_k), trong trường hợp này là số *k*.

Output: Ảnh Stego S có chứa thông điệp mật m.

Bước 1. Dùng thuật toán ZIP nén bản thông báo *M*, ta được ZIP(M) = X = (x_1, x_2,.., x_k);

Bước 2. Chuyển dãy ký tự X thành dãy nhị phân qua bộ mã ASCII, rồi chia kết quả thành từng block có độ dài bằng nhau và bằng 6, và kết quả được ký hiệu là

$X = (x_1, x_2, ..., x_{k/6})$, trong đó, $x_i = (x_{1,i}, x_{2,i}, ..., x_{6,i})$, $i = 1,2,..., [k/6]$ với [x] ký hiệu là phần nguyên của số x - là số nguyên lớn nhất nhưng không lớn hơn x, Ở đây, $x_{i,j} \in \{0,1\}$;

Bước 3. Trích chọn 63X [k/6] các LSB của các pixels dữ liệu của ảnh C bắt đầu từ một khởi điểm cho trước rồi gộp thành [k/6] block mỗi block có độ dài bằng nhau và bằng 63 bít, được ký hiệu là $Y = (y_1, y_2, ..., y_{k/6})$); trong đó, $y_i = (y_{1,i}, y_{2,i}, ..., y_{63,i})$, $i = 1,2,..., [k/6]$.

Bước 4. Với $i = 1,2,\ldots[k/6]$,

Tính $(z_i)^T = (x_i)^T + \mathbf{H}(y_i)^T$, ở đây là thực hiện phép cộng XOR;

Bước 5. Tìm xem trong Ma trận **H**, có cột nào trùng với $(z_i)^T$ hay không, nếu không thì giữ nguyên vecto y_i và trở lại Bước 4;

Bước 6. Giả sử, có tồn tại (sẽ là duy nhất) ở cột thứ j của ma trận **H** mà $(h_{.j})^T = (z_i)^T$ thì ta thực hiện đảo bít thứ j của vecto y_j thành $y_{j,i} + 1$, phép cộng ở đây là phép cộng không nhớ (XOR) rồi quay lại Bước 4;

Sau khi thực hiện xong cho đến khi $i = [k/6]$ thì chuyển sang Bước 7.

Bước 7. Trả lại toàn bộ tất cả các bít LSB đã sửa đổi theo đúng vị trí đã trích chọn ở Bước 3 từ khởi điểm giấu, ta nhận được ảnh Stego S.

- Thuật toán trích chọn:

Input: Ảnh S, ma trận **H** và khởi điểm giấu tin.

Output: Bản thông điệp M.

Bước 1. Xác định khởi điểm giấu và trích chọn theo thứ tự các LSB của các pixels của ảnh S cho đến k để nhận được dãy các bít $Z = (z_1, z_2, .., z_k)$;

Bước 2. Chia dãy Z thành từng block có độ dài bằng nhau và bằng 6, ta nhận được vecto $Y = (y_1, y_2, .., y_{[k/6]})$, trong đó, $y_i = (y_{1,i}, y_{2,i}, ..., y_{6,i})$, $i = 1,2,...,[k/6]$;

Bước 3. Với $i = 1,2..., [k/6]$,

Tính $(X_i)^T = \mathbf{H}(y_i)^T$;

Bước 4. Đổi dãy nhị phân $X = (X_1, X_2, .., X_k)$ sang các ký tự của ZIP qua bộ mã ASCII để nhận được các giá trị ban đầu của ZIP là $(x_1, x_2, x_3, ..., x_k)$;

Bước 5. Giải nén ZIP để nhận được bản thông báo M.

Chú ý: Nếu muốn khôi phục lại ảnh C, chúng ta có 2 cách thực hiện:

Cách 1. Trả lại toàn bộ các LSB đã trích chọn về vị trí ban đầu của chúng. Cách này có nhược điểm là thực tế đó là ảnh S chứ không phải là ảnh môi trường C

Cách 2. Dùng thông điệp đã trích chọn giấu lại lần thứ 2 theo đúng khởi điểm và đúng thuật toán giấu. Như vậy, sau khi giấu lần thứ 2 vào ảnh S các bít thông điệp giấu trong đó sẽ bị khử hết và như vậy ta nhận được ảnh C ban đầu.

[C4; 13-17].

3.4.3. Đánh giá độ an toàn thông tin được bảo mật

Trong bất cứ trường hợp nào, dữ liệu định vị đều mang tính bảo mật rất cao. Tính an toàn, bí mật, hiệu quả của việc bảo mật dữ liệu phụ thuộc vào hiệu quả của thuật toán giấu được so sánh với một số thuật toán khác dựa trên các tiêu chí như: tỉ lệ thông tin giấu, khả năng khó có thể phát hiện thông tin ẩn trong ảnh và tốc độ tính toán của thuật toán. Bài toán đặt ra: cần có sự đánh giá mức độ an toàn về mặt lý thuyết cho các hệ thống trên. Dựa trên các kết quả nghiên cứu về mặt toán học, luận án đề xuất phương pháp đánh giá độ an toàn cho mật mã và giấu tin như sau.

3.4.3.1. Cơ sở toán học

- Một số bổ đề của lý thuyết thông tin

Một số bổ đề của lý thuyết thông tin quan trọng đó là các Bổ đề 2 và Bổ đề 3 đã được trình bày và chứng minh ở trên. Trong đó Bổ đề 2 là chính là bổ đề cơ sở đánh giá độ an toàn của một Hệ thống thông tin có bảo mật.

- Một số cơ sở lý thuyết xác suất và thống kê toán học

Trong phạm vi phần trình bày, chúng tôi chỉ tập trung xây dựng đánh giá mức độ an toàn thông tin đối với hệ thống mật mã và hệ thống kỹ thuật giấu tin trong ảnh số. Đối với hệ mật mã, phần trình bày chỉ tập trung xem xét đánh giá hệ mật mã dòng. Đối với một hệ thống mật mã dòng, độ an toàn của nó là chất lượng của dãy giả ngẫu nhiên được mầm khóa sinh ra. Nghĩa là các bit của dãy được thiết bị sinh tạo ra là

độc lập và có phân bố xác suất đồng đều, nghĩa là dãy đó gần với dãy ngẫu nhiên. Trước hết, ta có bổ đề sau đây.

Bổ đề 4. Cho hai đại lượng X_1, X_2 độc lập có hàm mật độ lần lượt là $P_1(.)$ và $P_2(.)$ trên không gian S. Đặt $\eta = X_1 + X_2$

Khi đó, đại lượng ngẫu nhiên η có hàm mật độ là

$$p_\eta(x) = \int_S P_1(y)P_2(x-y)dy$$

Hệ quả 1. Cho X_1, X_2 là hai đại lượng ngẫu nhiên, độc lập, rời rạc: X_1 nhận các giá trị $x_1, x_2, .., x_k$ với xác suất tương ứng là $p_1, p_2, .., p_k$; $\left(p_i = \left(X_1 = x_i\right), i = 1, .., k\right)$

X_2 nhận các giá trị $x_1, x_2, .., x_k$ với các xác suất tương ứng là $q_1, q_2, .., q_k$ $\left(q_i = p(X_2 = x_i) i = 1,2, .., k\right)$

Đặt $Z = X_1 + X_2$. Khi đó, đại lượng ngẫu nhiên Z sẽ nhận các giá trị $Z_1, Z_2, .., Z_K$ với xác suất tương ứng là:

$$r_j = p(Z_j) = \sum_{i=1}^{K} p_i q_{j-i} \text{ với } p_i = p(X_1 = x_i);\ q_{j-i} = p(X_2 = Z_j - x_i);\ j = 1,2, ..k$$

Hệ quả 2. Cho hai đại lượng ngẫu nhiên X_1, X_2 thỏa mãn các điều kiện của Hệ quả 1. Nếu một trong hai (chẳng hạn X_1) đại lượng ngẫu nhiên đó có phân bố đều $P_1 = P_2 = ...P_k = \frac{1}{2}$. Đại lượng ngẫu nhiên Z cũng có phân bố đều, nghĩa là $r_1 = r_2 = ... = r_k = \frac{1}{k}$

Chứng minh. Thật vậy, áp dụng kết quả của Hệ quả 1, ta có với $j = 1,2, .., k$,

$$r_j = \sum_{i=1}^{k} p_i q_{j-i} = \sum_{i=1}^{k} p(X_1 = x_i) p(X_2 = Z_j - x_i) = \frac{1}{k} \sum_{i=1}^{k} p\left(Z_2 = Z_j - x_i\right) = \frac{1}{k}$$

Hệ quả được chứng minh.

- Độ an toàn của hệ thống

Để đánh giá độ an toàn của một hệ thống mật mã, chúng ta cần đánh giá chất lượng ngẫu nhiên của dãy giả ngẫu nhiên do hệ thống sinh (gmerator) tạo ra. Đầu ra đó có thể là dãy các chữ cái La tinh, dãy số tự nhiên hoặc dãy nhị phân. Việc đánh

giá này liên quan đến bài toán kiểm định các giả thuyết thống kê toán. Nội dung bài toán như sau: Giả sử trên cơ sở nào đó, người ta đưa ra hai giả thuyết thống kê đối lập nhau, lần lượt được ký hiệu là giả thuyết H_0 và đối thuyết H_1. Ví dụ:

H_0: Hệ thống sinh dãy giả ngẫu nhiên độc lập có phân bố xác suất đều.

Trái lại:

H_1: Hệ thống đó sinh dãy giả ngẫu nhiên độc lập nhưng có phân bố không đều. Để kiểm tra xem giả thuyết nào đúng trong hai giả thuyết đưa ra, ta lấy mẫu giả ngẫu nhiên $X = x_1, x_2, .., x_n$ $(n \geq 2)$ rồi tính đặc trưng phân bố xác suất của X. Nếu đặc trưng đó tương ứng với giả thuyết không thì ta chấp nhận giả thuyết H_0 và do đó bác bỏ giả thuyết H_1. Ngược lại thì ta chấp nhận giả thuyết H_1 và bác bỏ giả thuyết H_0.

Trong bất cứ một chiến lược quyết định nào, chúng ta đều mắc phải hai sai lầm: Sai lầm xảy ra khi H_0 đúng, nhưng ta lại quyết định bác bỏ nó, được gọi là xác suất sai lầm loại một và được ký hiệu là α $(0 \leq \alpha \leq 1)$ và xác suất sai lầm loại hai được ký hiệu là β là sai lầm xảy ra khi chấp nhận giả thuyết sai $(0 \leq \beta \leq 1)$

Trong thực tế chúng ta không có quyết định nào mà cực tiểu hóa đồng thời cả hai sai lầm loại 1 và loại 2. Do đó một quyết định được cho là tối ưu nếu cố định xác suất sai lầm loại một α cho trước mà cực tiểu hóa sai lầm loại hai β. Bài toán đó đã được nghiên cứu nhiều trong lý thuyết kiểm định giả thuyết thống kê và không phải là mục tiêu của phần này.

Phần sau đây đánh giá mức độ an toàn của hệ thống mật mã dựa trên cơ sở xích Markov hữu hạn trạng thái. Để đánh giá chất lượng của các bản mã do hệ thống sinh tạo ra, ta sẽ đánh giá chất lượng các dãy giả ngẫu nhiên được dùng để mã hóa các bản thông báo một dãy dãy giả ngẫu nhiên được sinh từ hệ thống nào đó được coi là tốt nếu các thành phần của dãy đó là độc lập và có phân bố đều. Như vậy, một dãy giả ngẫu nhiên hoàn toàn độc lập và có phân bố đều là dãy thuộc xích markov với ma trận chuyển trạng thái là $P = (P_{ij})_{m \times m}$ trong đó m là số trạng thái khác nhau của xích. Trường hợp đặc biệt nhưng quan trọng là $m = 26$ (tương ứng với 26 chữ cái la tinh)

và $P_{ij} = \frac{1}{26}$, đối với mọi $i, j = 1,2,..,26$. Như vậy, P là ma trận vuông cấp 26×26 với các phần tử bằng nhau và bằng $\frac{1}{26}$.

Một dãy giả ngẫu nhiên được cho là tồi nếu dãy đó vi phạm các tiêu chuẩn thống kê về tính độc lập và phân bố đều.

Như vậy, bài toán kiểm định giả thuyết H_0 và theo dõi giả thuyết H_1 như sau:

H_0: Hệ thống sinh dãy giả ngẫu nhiên theo mô hình Markov với ma trận chuyển $P_0 = \left(\frac{1}{26}\right)_{26\times 26} = \left(P_{ij}\right)_{26\times 26}$

H_1: Hệ thống sinh dãy giả ngẫu nhiên theo mô hình Markov $q_1 = \left(q_{ij}\right)_{26\times 26}$, trong đó q_{ij} cho trước hoặc ước lượng được bằng phương pháp thống kê toán học. Ở đây chúng tôi sử dụng phương pháp cực đại hợp lý (maximal likelihood estimation). Trong thực hành, ta lấy mẫu khoảng 10000 chữ cái la tinh. Vì vậy, để đơn giản cho tính toán, trong thực hành ta lấy $p_{ij} = \frac{10000}{26^2} \approx 14{,}80$ đối với mọi $i, j = 1,2,..,26$. Còn $\left(q_{ij}\right)_{26\times 26}$ đã được tính toán và cho kết quả.

3.4.3.2. Đánh giá độ an toàn của hệ thống thông tin được bảo mật

<u>Định nghĩa</u>: Độ an toàn hoàn hảo.

Cho Ω là một hệ thống thông tin (Steganography). $P_S(.)$ là phân bố xác suất của ảnh stego khi gửi qua kênh công cộng và $P_C(.)$ là phân bố xác suất của ảnh cover (ảnh chứa giấu tin) chúng thường được gọi là ảnh môi trường. Khi đó hệ thống Ω được gọi là ε_an toàn chống lại các tấn công bị động nếu và chỉ nếu $D\left(P_S \| P_C\right) \le \varepsilon$ với $\varepsilon \ge 0$ cho trước.

Hệ thống Ω được gọi là có độ an toàn hoàn hảo (perfect secutity) nếu $\varepsilon = 0$ .Trong đó, $D\left(P_1 \| P_2\right) = \sum_{q \in Q} P_1(p) \log \frac{P_1(q)}{P_2(q)}$

Vì $D(P_S \| P_C) = 0 \Leftrightarrow$ phân bố xác suất của ảnh stego S bằng phân bố xác suất của ảnh Cover C tương ứng, tức là kẻ tấn công không phân biệt được đâu là ảnh gốc C và đâu là ảnh có chứa thông tin mật (ảnh stego S)

Ta có định lý sau đây:

Định lý 2: Có tồn tại một hệ thống steganography có mức an toàn hoàn hảo.

Chứng minh: Cho C là tập hợp tất cả các dãy nhị phân có độ dài n, P_C là phân bố xác suất đều trên C và lấy $m \in C$ là một bản tin rõ (message). Bây giờ người gửi lấy ngẫu nhiên $c \in C$ rồi tính $s = c \oplus m$. Ta có $P_S(.) = P_C(.)$ và do đó theo Bổ đề 1 ta suy ra $D(P_S \| P_C) = 0$.

Hệ thống steganography nêu trên rất đơn giản nhưng thường không dùng trong thực tế vì như vậy A và B trao đổi dãy ngẫu nhiên cho nhau (chứ không phải bản rõ).

Định lý 3: Cho Ω là một hệ thống steganography ε- an toàn chống lại các tấn công bị động, β là xác suất mà kẻ tấn công không phát hiện ảnh chứa thông điệp ẩn và α là xác suất để kẻ tấn công phát hiện sai ảnh có chứa thông điệp sẽ thỏa mãn: $d(\alpha, \beta) \le \varepsilon$, trong đó $d(\alpha, \beta) = \alpha \log_2 \frac{\alpha}{1-\beta} + (1-\alpha) \log_2 \frac{1-\alpha}{\beta}$ với $(0 \le \alpha, \beta < 1)$

Đặc biệt, nếu $\alpha = 0$, khi đó $\beta \ge 2^{-\varepsilon}$.

Bổ đề 5. Giả sử X, Y là đại lượng ngẫu nhiên được xác định trên tập S với phân bố xác suất lần lượt là $P_X(.)$ và $P_Y(.)$; f là một ánh xạ $f : S \to T$

Khi đó, $D(P_{T_0} // P_{T_1}) \le D(P_X // P_Y)$, trong đó P_{T_0} và P_{T_1} ký hiệu là các phân bố xác suất của $f(X)$ và $f(Y)$

Từ định lý 2 và 3 cùng các kết quả trong Bổ đề 5, lấy $\varepsilon = 0{,}05$ và $\alpha = 0$ thì $\beta \ge 2^{-0{,}05} = \frac{1}{2^{0{,}05}} \approx 0{,}97$

Nghĩa là hệ thống an toàn với $\varepsilon = 0{,}05$ thì kẻ tấn công khó có thể dò tìm ảnh chứa thông tin ẩn (xác suất $\ge 97\%$).

3.4.3.3. Thực nghiệm

- Đối với hệ thống steganography

Cho C là ảnh cover, còn S là ảnh stego đã được giấu thông điệp với tỉ lệ nào đó và cho trước $\varepsilon = 0{,}1$

Bước 1. Trích chọn n bit LSB của ảnh cover C và n bit LSB của ảnh stego S tương ứng (cùng khởi điểm giấu). Ta nhận được kết quả lần lượt là:

$c_1c_2...c_n$ và $s_1s_2...s_n$; $c_i, s_i \in \{0,1\}; i = 1,2,..,n$

Bước 2. Tính tần số bộ đôi móc xích lần lượt của 2 dãy $\{c_1c_2..c_n\}$ và $\{s_1s_2..s_n\}$ ta được kết quả $P_C(x)$ và $P_S(x)$ như sau:

$$P_C = \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix} \qquad P_S = \begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}$$

Bước 3. Tính $D(P_C // P_S) = \sum_{i=1}^{2}\sum_{j=1}^{2} P_C(i,j)\log_2 \frac{P_C(i,j)}{P_S(i,j)}$

Trong đó, $P_C(i,j) = p_{ij}$; $i, j = 1,2$; $P_S(i,j) = q_{ij}$; $i, j = 1,2$

Bước 4. Nếu $D(P_C // P_S) \le 0{,}1$ thì hệ thống là đáng tin cậy và thuật toán dừng.

Bước 5. Hệ thống không đáng tin cậy (với mức an toàn 95%).

- Đối với hệ thống sinh bit giả ngẫu nhiên tùy ý

Thuật toán 1: Cho một dãy bít giả ngẫu nhiên được sinh từ hệ thống sinh nào đó: $X = x_1x_2...x_n$; $x_i \in \{0,1\}$; $i = 1,2,..,n$. Vẫn chọn $\varepsilon = 0{,}1$

Bước 1. Tính tần số bộ đôi móc xích của dãy X và nhận được kết quả $P = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$

Bước 2. Tính $Q = (q_{ij})_{2\times 2}$ trong đó $q_{ij} = \left[\log_2 \frac{n}{4m_{ij}}\right]$

Bước 3. Tính $S(x) = \sum_{1}^{2}\sum_{1}^{2} \frac{n}{4} q_{ij}$

Bước 4. Nếu ε = 0,05 thì hệ thống có độ an toàn tốt với xác suất 97% và hệ thống dừng. Trái lại,

Bước 5. Hệ thống không an toàn và thuật toán dừng (termirate algorithm).

Thuật toán 2: Ta có định lý sau:

Cho dãy nhị phân $X = x_0 x_1 ... x_{n-1}$, độ dài n

Lấy và cố định số nguyên d : $1 \le d \le \lfloor n/2 \rfloor$ (phần nguyên của n/2).

Đặt $A(d) = \sum_{i=0}^{n-d-1} (x_i \oplus x_{i+d})$. Nếu $n-d \ge 10$, ta có: $\lambda = \left(2\left(A(d) - \frac{n-d}{2} \right) \right) / \sqrt{n-d}$ sẽ có phân bố xấp xỉ phân bố chuẩn $N(0,1)$.

Điều này có nghĩa là: Cho trước xác suất sai lầm loại 1, giả sử lấy $\alpha = 0,05$. Khi đó tra bảng phân phối chuẩn ta xác định được ngưỡng $t_\alpha = 1,6449$ [xem 1].

Khi đó nếu $2\left(A(d) - \frac{n-d}{2} \right) < t_\alpha \sqrt{n-d} = 1,6449\sqrt{n-d}$ thì ta chấp nhận dãy X là tốt; trái lại thì ta coi dãy X được sinh ra từ bộ sinh là không tốt.

- Đối với dãy giả ngẫu nhiên chữ cái Latinh

Xét trên bảng chữ cái La tinh $Z_{26} = \{a, b, c, .., z\}$ hay $= \{0,1,2,3,..,25\}$

Tiếp theo, lấy 2 mẫu văn bản tiếng Anh tùy ý một cách độc lập, mỗi mẫu X, Y có độ dài như nhau và bằng n (cỡ 10000 chữ cái) mà ta ký hiệu là

$X = x_1, x_2, .., x_n$

$Y = y_1, y_2, .., y_n$

Bước 1. Cộng $(x + y) \bmod 26 = Z = z_1, z_2, .., z_n$

Bước 2. Tính tần số bộ đôi móc xích của dãy Z, ta được kết quả $G = (g_{ij})_{26 \times 26}$

Bước 3. Tính $H = (h_{ij})_{26 \times 26}$. Trong đó, $h_{ij} = \left[K \log \frac{0,0015n}{g_{ij}} \right]$; $i, j = 1,2,..,26$

Với K là một số nguyên dương nào đó $(K \ge 1)$. Trong thực hành, chúng ta chọn $K = 10$. Mục đích chọn số K là làm tăng độ chính xác của kết luận, tức là giảm thiểu trường hợp $[\log x] = 0$. Chẳng hạn lấy $x = 1,2$ và logarit là ln. Khi đó: $[\ln 1,2] = [0,1820] = 0$. Tuy nhiên $[10 \ln 1,2] = [1,820] = 1$

Bây giờ giả sử ta cần kiểm tra một dãy sinh $S = s_1 s_2 .. s_m$ với $m \ge 1$; $s_i \in \{a, b, .., z\}$; $i = \overline{1, m}$

Bước 1. Tính tần số bộ đôi móc xích của dãy S, ta nhận được kết quả là ma trận Q

$Q = (q_{ij})_{26\times 26}$; $q_{ij} \geq 0$; $i, j = 1,2,..,m$

Bước 2. Tính vết $Tr(Q.H^T)$, trong đó H^T là ma trận chuyển vị của ma trận H

Bước 3. Nếu giá trị $Tr(Q.H^T) > 0$ thì dãy S được sinh ra từ bộ sinh dãy giả ngẫu nhiên nào đó là tốt.

Trái lại nếu $Tr(Q.H^T) < 0$ thì dãy S là không tốt và thuật toán dừng. Trường hợp $Tr(Q.H^T) = 0$ thì chưa có kết luận mà ta cần lấy tiếp mẫu S có độ dài lớn hơn m và tiếp tục quay về Bước 1.

Bước 4. Bổ sung thêm mẫu s thành s' để có độ dài $m' > m$ và quay lại Bước 1.

[C1, 13-17].

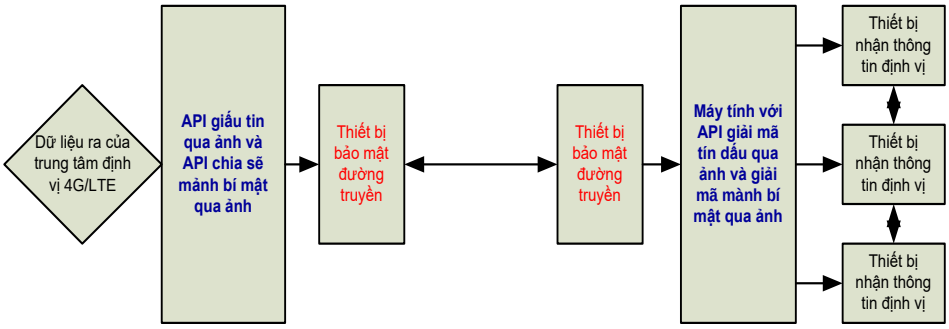
3.4.4. Đề xuất hệ thống kỹ thuật bảo mật chuyển giao kết quả định vị

Với yêu cầu bảo mật chuyển giao kết quả định vị đến một nhóm người dùng hoặc một người dùng khi không có sẵn môi trường truyền thông an toàn, căn cứ vào kết quả nghiên cứu ở trên, luận án đề xuất hệ thống kỹ thuật bảo mật sử dụng phương pháp cơ bản như sau:

- Chuyển giao kết quả định vị đến một nhóm người dùng cần sử dụng chung, duy nhất một kết quả định vị bằng phương pháp chia sẻ mảnh bí mật qua ảnh của chính các người dùng trong nhóm. Chỉ khi mỗi người dùng trong nhóm nắm được khóa mã mới ghép được các mảnh bí mật với nhau trở thành kết quả rõ.
- Chuyển giao kết quả định vị đến một người dùng bằng áp dụng phương pháp giấu tin qua ảnh. Chỉ khi người dùng có khóa mã mới có được kết quả rõ.

3.4.4.1. Sơ đồ cấu trúc hệ thống

Căn cứ vào phương pháp đã nêu ở trên, hệ thống kỹ thuật bảo mật chuyển giao kết quả định vị có cấu trúc như sau:



Hình 3. 4. Sơ đồ hệ thống kỹ thuật bảo mật chuyển giao kết quả định vị

3.4.4.2. Mô tả chức năng hệ thống

Trước khi được đưa vào đường truyền, dữ liệu kết quả định vị được trung tâm định vị đưa vào một trong hai API, hoặc là API giấu tin mật qua ảnh hoặc là API chia sẻ mảnh bí mật qua ảnh. Tại đầu nhận, tùy theo yêu cầu, người nhận sẽ sử dụng một trong hai API giải mã ảnh chứa thông tin mật để lấy ra thông tin rõ hoặc lấy ra từng mảnh thông tin rõ và ghép thành bản thông tin rõ đầy đủ.

3.5. Giải pháp kỹ thuật giả lập trạm gốc thu thập tham số IMSI/IMEI

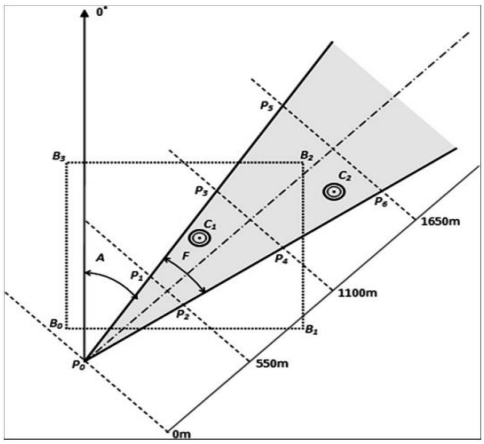
3.5.1. Yêu cầu

Yêu cầu tìm kiếm, phát hiện và định vị chính xác một thiết bị di động phục vụ công tác an ninh nói chung và công tác cứu hộ, cứu nạn ngày càng cao. Các đối tượng hoặc mục người cần cứu hộ, cứu nạn thường mang theo điện thoại di động (hay một thiết bị di động). Tuy nhiên, vì nhiều lý do khác nhau mà không biết họ, tức thiết bị di động đó có xuất hiện tại khu vực nghi ngờ hay không và vị trí chính xác là ở đâu. Trong nội dung này, luận án đề xuất giải pháp kỹ thuật nhằm phát hiện một thuê bao (máy di động, thiết bị di động) có xuất hiện tại khu vực nghi ngờ hay không để hỗ trợ tìm kiếm, xác định vị trí của nó.

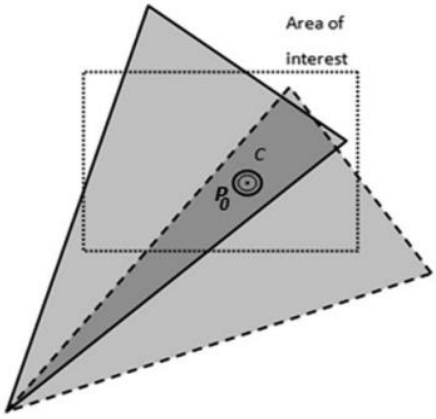
3.5.2. Đề xuất giải pháp kỹ thuật

IMSI (số nhận dạng thuê bao di động quốc tế), là một số nhận dạng duy nhất cho mỗi thuê bao điện thoại di động GSM/UMTS/4G LTE trên toàn thế giới. IMSI được chứa trong thẻ SIM của điện thoại. IMSI thường là một chuỗi 15 chữ số, gồm một MCC (Mã di động quốc gia), một MNC (Mã mạng di động) và một MSIN (Số

nhận dạng trạm di động). IMEI (số nhận dạng thiết bị di động quốc tế), là một dãy số duy nhất xác định một chiếc máy điện thoại di động trên toàn thế giới. IMEI dùng để tra cứu thông tin trên máy di động và xác thực tính hợp lệ của chiếc máy đó (ví dụ máy bị đánh cắp mà dùng SIM khác thì có thể bị mạng di động đưa vào danh sách đen, không phục vụ). Tuy nhiên, vì lý do bảo mật, tham số IMSI và IMEI bị hạn chế truyền trên giao diện vô tuyến, và thay vào đó mạng sử dụng số nhận dạng thuê bao di động tạm thời (TMSI) được tạo ra một cách ngẫu nhiên và chỉ tồn tại trong thời gian ngắn để tránh bị theo dõi và làm lộ danh tính người dùng. Thay vào đó, IMSI/IMEI chỉ được sử dụng trong một số trường hợp nhất định như lần đầu đăng nhập vào mạng, trả lời yêu cầu xác thực thuê bao của mạng. Đặc biệt đối với mạng 4G-LTE, tham số IMEI chỉ được truyền trên giao diện vô tuyến khi đã xác thực hai chiều giữa UE và mạng. Do tính duy nhất của tham số IMSI/IMEI, nên bằng cách nào có thể thu được tham số này, sẽ biết rằng có sự xuất hiện của thuê bao điện thoại di động tại khu vực nghi ngờ. Trên cơ sở đó, luận án đề xuất giải pháp phát hiện sự xuất hiện của thuê bao điện thoại cần tìm bằng cách thu thập tham số IMSI/IMEI của điện thoại di động bởi một trạm gốc giả lập. Khoảng cách và khu vực thu thập tham số IMSI/IMEI hiệu quả có thể thay đổi thông qua thay đổi công suất phát của trạm giả và độ định hướng của ăng ten, cho phép khoanh vùng hẹp khu vực hoạt động của điện thoại, như thể hiện tại các hình sau đây.



Hình 3. 5. Phạm vi khu vực thu thập được tham số IMSI/IMEI (C1, C2)



Hình 3. 6. Góc và hướng của trạm giả có thể thay đổi để xác định khu vực hẹp của mục tiêu

Để thu được tham số này, cần có một thiết bị thu phát sóng trung gian đứng giữa, sao cho thiết bị này hoạt động như một trạm gốc di động thật và thuê bao di động cần tìm sẽ tự động đăng ký và hoạt động trên mạng cục bộ do thiết bị trung gian đó tạo ra. Khi đó, thiết bị trung gian được gọi là trạm gốc giả lập. Phương thức này được gọi là MITM (Man in The Middle – Người đứng giữa) và thiết bị đó gọi là Trạm gốc giả lập (Clone BTS/eNB) hay Bộ chặn bắt tham số (IMSI Catcher). Để có thể tham gia vào quá trình xác thực và thu thập được tham số IMSI/IMEI, trạm gốc giả lập sẽ được thiết lập cấu hình, tính năng như trạm gốc thật của nhà mạng. Từ đó, máy di động sẽ bị buộc đăng ký vào mạng qua trạm giả lập, thực hiện các giao dịch qua trạm giả đó và trạm giả sẽ thu nhận được tham số IMSI/IMEI của nó. Cách thức hoạt động và nguyên lý kỹ thuật thu thập tham số IMSI/IMEI bằng trạm gốc giả lập như sau:

*** Đối với mạng 2G**

Một trong những điểm yếu của GSM (2G) là việc chỉ có xác thực một chiều của nhà mạng đối với điện thoại, điện thoại không xác thực các thành phần của mạng. Điều đó có nghĩa là một người dùng của mạng A khi bật điện thoại lên sẽ phải xác thực trước khi gia nhập mạng A, tuy nhiên người dùng sẽ không xác thực xem mạng A có đúng là mạng A hợp pháp hay không. Do vậy, một bộ trạm gốc giả lập có thể thu thập được tham số của máy di động nếu nó đăng ký, kết nối qua trạm giả lập này. Cơ chế hoạt động như sau*:*

- Bước 1. Thiết lập một trạm thu phát sóng giả nằm cùng vùng với trạm thu phát sóng hợp pháp.

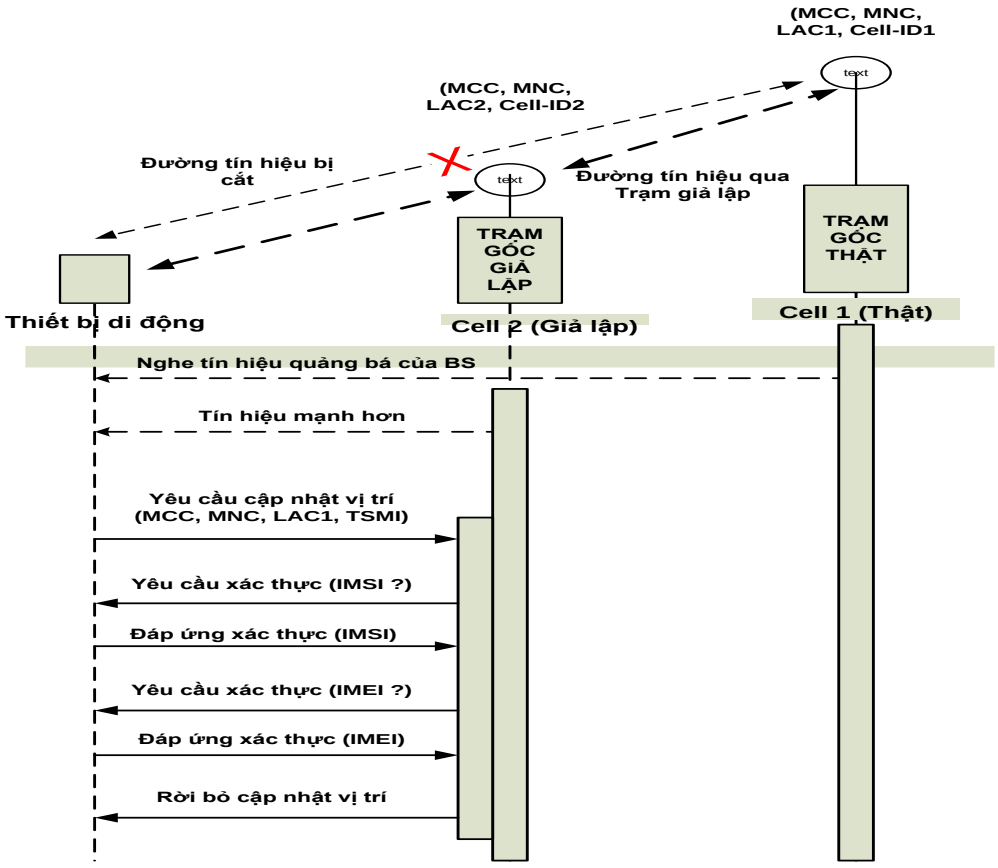
- Bước 2. Dùng các phương pháp khác nhau để bắt các thiết bị di động trong vùng phủ sóng thiết lập kết nối với trạm phát sóng giả thay vì với trạm phát sóng hợp lệ.

Điện thoại di động thông qua việc đọc bản tin quảng bá của trạm di động xung quanh, phát hiện và xếp hạng các trạm có tín hiệu mạnh nhất để thực hiện kết nối. Các tiêu chí, thuật toán để xếp hạng tế bào được mô tả trong thủ tục lựa chọn, tái lựa chọn tế bào.Trạm giả cố gắng phát tín hiệu có cường độ mạnh nhất, với thông số mã định danh khu vực vị trí (LAC) khác với trạm thực trong khu vực, nhằm kích hoạt thủ tục “Cập nhật vị trí với tham số TMSI”. Đến đây, trạm giả sẽ phản hồi tới điện

thoại bằng thủ tục "Yêu cầu nhận thực bằng IMSI/IMEI", nhận được yêu cầu này bắt buộc điện thoại phải phản hồi trạm giả tham số IMSI/IMEI tương ứng.

- Bước 3. Sau khi đạt được mục đích thu chặn IMSI/IMEI của điện thoại di động, trạm giả thực hiện giao thức "Rời bỏ thủ tục cập nhật vị trí".

Hình sau đây mô tả cơ chế thu chặn chủ động thu thập tham số IMSI/IMEI trong mạng 2G.



Hình 3. 7. Cơ chế thu chặn chủ động thu thập tham số IMSI/IMEI mạng 2G

**** Đối với mạng 3G và 4G:***

Có hai phương pháp thực hiện, cụ thể như sau:

- Phương pháp 1:

Bởi có sự tồn tại đồng thời của mạng 2G trong môi trường 3G/4G và các mạng có cơ chế lựa chọn tế bào liên mạng nên có thể sử dụng thiết bị gây nhiễu làm cho điện thoại đang từ 3G/4G "rơi" xuống hoạt động ở 2G. Cơ chế hoạt động của phương pháp này như sau:

- Bước 1. Thiết lập trạm gây nhiễu với cường độ tín hiệu phù hợp có thể làm mất sóng toàn bộ tín hiệu 3G/4G hoặc làm giảm cường độ tín hiệu của trạm 3G/4G đến một ngưỡng nhất định đáp ứng điều kiện kích hoạt thủ tục chuyển giao liên RAT và tái lựa chọn lại tế bào trên trạm giả 2G.

- Bước 2. Thực hiện các thủ tục tương tự như đã nêu phần giả trạm 2G để thu thập tham số IMSI/IMEI của điện thoại di động.

**** Phương pháp 2:***

- Bước 1. Triển khai trạm phát sóng giả 3G/4G cùng với khu vực trạm phát sóng hợp pháp.

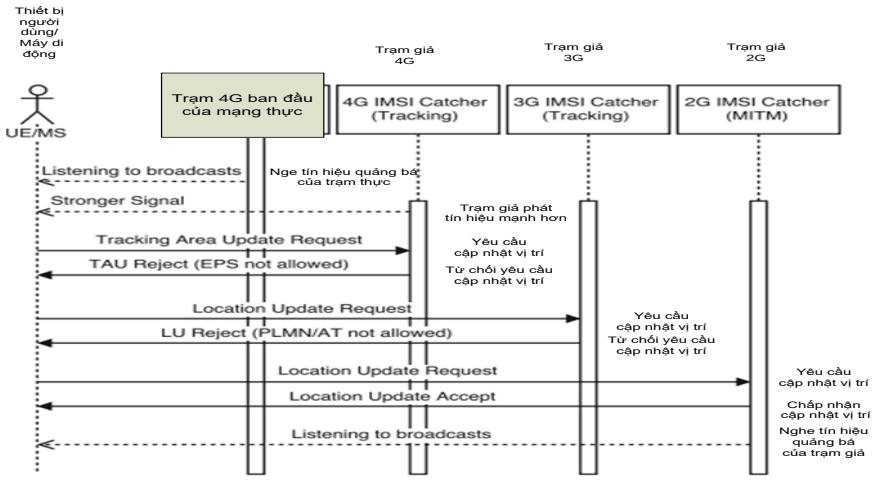
- Bước 2. Bằng các phương pháp khác nhau để bắt điện thoại thực hiện thủ tục cập nhật vị trí với tham số định danh tạm thời TMSI.

- Bước 3. Trạm giả trả lời điện thoại bằng bản tin từ chối cập nhật vị trí với nguyên nhân lỗi (trong 4G: EPS not allowed; 3G: PLMN/AT not allowed).

Khi nhận được các nguyên nhân lỗi như được mô tả bên trên, theo quy định của tiêu chuẩn di động, điện thoại di động sẽ không được phép truy cập vào các dịch vụ của mạng 3G/4G tương ứng. Nó bắt buộc phải thực hiện lại thủ tục tìm kiếm tế bào mới trên mạng 2G.

- Bước 4. Thực hiện thu chặn tham số IMEI/IMSI như trong trường hợp 2G.

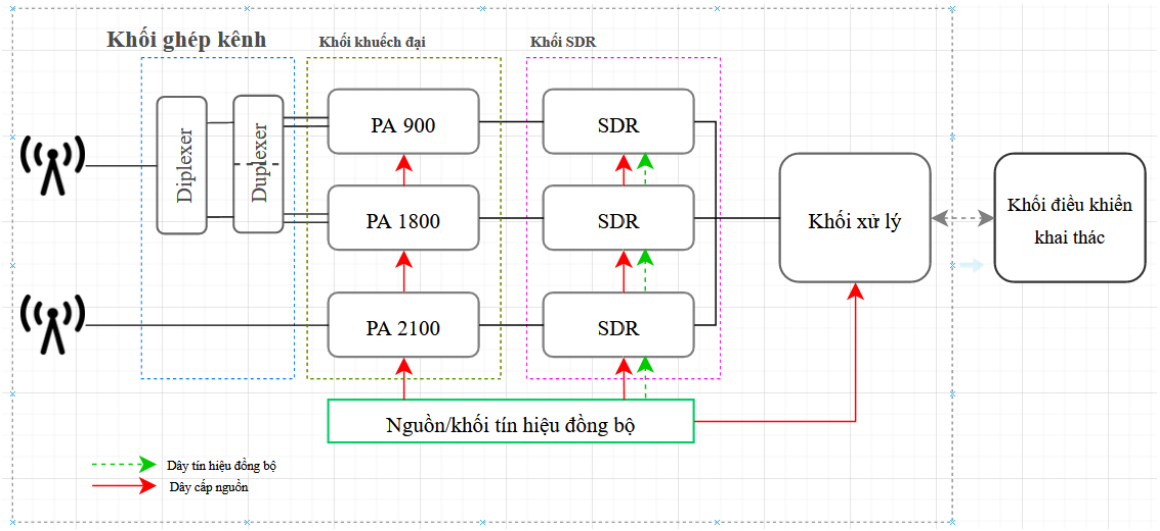
Hình sau đây mô tả phương pháp thu thập tham số IMSI/IMEI bằng yêu cầu thủ tục tái tìm kiếm tế bào liên mạng 4G/3G-2G.



Hình 3. 8. Cơ chế thu thập tham số IMSI/IMEI bằng yêu cầu thủ tục tái lựa chọn tế bào liên mạng 4G/3G-2G

3.5.3. Sơ đồ cấu trúc trạm gốc giả lập

Trên cơ sở giải pháp kỹ thuật nêu trên, căn cứ vào số liệu tần số của mạng Việt Nam, luận án đề xuất sơ đồ cấu trúc trạm gốc giả lập 3 băng tần 2G/3G/4G điển hình (cho mạng Vinaphone) như hình dưới đây:



Hình 3. 9. Sơ đồ cấu trúc thiết bị giả lập trạm gốc 3 băng tần 2G/3G/4G [J3, 46-54].

3.6. Kết luận Chương 3

Căn cứ vào giải pháp kỹ thuật đã lựa chọn ở Chương 2, trong Chương 3, luận án đã đề xuất mô hình kiến trúc tổng thể hệ thống định vị thiết bị di động trên cơ sở sử dụng phân lớp, xác định đối tượng định vị; bảo mật chuyển giao kết quả định vị; trạm gốc giả lập thu thập tham số IMSI/IMEI hỗ trợ tìm kiếm, định vị đối tượng. Mô hình hệ thống kỹ thuật đã nêu trên đáp ứng yêu cầu của bài toán định vị thiết bị di động thế hệ thứ tư phục vụ công tác an ninh. Với mô hình hệ thống kỹ thuật được đề xuất, CQAN có thể ứng dụng để xây dựng một hệ thống kỹ thuật tổng thể, hiệu quả, khả thi cho yêu cầu định vị thiết bị di động thế hệ thứ tư phục vụ công tác.

CHƯƠNG 4. THỰC NGHIỆM

Chương 4 của Luận án sẽ trình bày một số thực nghiệm để minh chứng giải pháp kỹ thuật và mô hình hệ thống định vị được nghiên cứu, đề xuất tại Chương 2 và Chương 3. Nội dung sau đây sẽ trình bày sơ đồ, kịch bản, kết quả và đánh giá về các thực nghiệm:

- Thu thập dữ liệu Cell-ID từ nguồn mở.
- Cải thiện độ chính xác kỹ thuật định vị ToA, AoA.
- Giả lập trạm gốc thu thập tham số IMSI/IMEI, xác định vị trí tương đối (hẹp) của đối tượng; đánh giá sự thay đổi công suất trạm giả lập với cự ly, khoảng cách thu được tham số IMSI/IMEI.
- Tìm hướng, định vị tầm gần đối tượng bằng trạm gốc giả lập.

4.1. Thu thập dữ liệu Cell-ID từ nguồn mở

4.1.1. Phân tích các phương pháp thu thập dữ liệu Cell-ID

Để định vị di động và biểu diễn kết quả trên bản đồ, trước hết chúng ta phải có cơ sở dữ liệu Cell-ID của các nhà mạng di động. Có 3 cách thu thập cơ sở dữ liệu Cell-ID:

- Dùng thiết bị cơ động đo mạng di động để lấy dữ liệu của từng Cell cần biết.
- Thu thập từ cơ sở dữ liệu của các nhà mạng bằng cách truy cập trực tuyến hoặc không trực tuyến bởi các tập dữ liệu Cell-ID do nhà mạng cung cấp.
- Thu thập từ nguồn mở.

Về cơ bản, cần phải thực hiện cả 3 phương pháp trên. Phương pháp thứ nhất và thứ hai có nhiều khó khăn, hạn chế trong thực tế. Ví dụ, phương pháp dùng máy đo mạng để lấy dữ liệu chỉ có thể thực hiện được ở những địa điểm, khu vực trọng điểm vì số lượng Cell của các nhà mạng là rất lớn. Phương pháp kết nối, lấy dữ liệu từ nhà mạng không phải lúc nào cũng có sẵn vì các vấn đề liên quan đến quy định của pháp luật, chính sách bảo mật kinh doanh của nhà mạng, sự thay đổi thường xuyên liên tục cấu trúc Cell của mạng. Phương pháp thu thập từ nguồn mở có thuận

lợi cơ bản là cơ quan an ninh sẽ chủ động hơn và có thể thu thập, cập nhật, làm giàu cơ sở dữ liệu một cách trực tuyến, thường xuyên, miễn phí.

Qua nghiên cứu, khảo sát nhận thấy có hai nguồn mở dữ liệu Cell-ID có thể sử dụng như sau:

- Cơ sở dữ liệu nguồn mở OpenCellID:

OpenCellID là dự án cộng đồng lớn nhất trên thế giới thu thập các vị trí GPS của BTS/eNB, được sử dụng miễn phí, cho các mục đích thương mại và tư nhân. Hiện có hàng trăm ngàn người đăng ký, vừa sử dụng dữ liệu vừa cập nhật dữ liệu, đóng góp trung bình hàng triệu phép đo mới mỗi ngày cho cơ sở dữ liệu OpenCellID. Tính đến nay, cơ sở dữ liệu mở này chứa gần 100 triệu Cell-ID. OpenCellID cung cấp dữ liệu Cell-ID 100% miễn phí (dưới Giấy phép Quốc tế Creative Commons Attribution-ShareAlike 4.0). Cơ sở dữ liệu OpenCellID có tính chất mở với mục đích thúc đẩy việc sử dụng và phân phối lại dữ liệu miễn phí.

- Cơ sở dữ liệu Cell-ID của Google:

Cơ sở dữ liệu này để phục vụ dịch vụ dẫn đường Google Maps. Dịch vụ dẫn đường của Google được sử dụng rộng rãi trên toàn thế giới nhưng cơ sở dữ liệu này không phổ biến rộng rãi và ít người biết. Thực tế sử dụng Google Maps trên thế giới cho thấy cơ sở dữ liệu này là rất lớn, tin cậy, ngày càng chính xác.

4.1.2. Thu thập dữ liệu Cell-ID từ nguồn mở OpenCellID

4.1.2.1. Phương pháp

Việc thu thập dữ liệu Cell-ID từ nguồn mở OpenCellID được thực hiện theo các bước sau:

- Bước 1. Xác định vùng địa lý bất kỳ cần thu thập dữ liệu Cell-ID
- Bước 2. Thực hiện lệnh yêu cầu Request API tới OpenCellID.
- Bước 3. Xử lý dòng dữ liệu trả về (response) bằng kỹ thuật Response Stream Reader để nhận được danh sách các Cell trong khu vực với dữ liệu của nó.
- Bước 4. Sắp xếp dữ liệu trên bảng và biểu diễn dữ liệu trên bản đồ số.

4.1.2.2. Thực nghiệm và kết quả

Thực hiện các bước 1-3 trên bằng lệnh có sẵn của OpenCellID, ví dụ thực hiện dòng lệnh yêu cầu như sau:

http://OpenCellID.org?APIKey=<Key>Box=<Area>

Trong Request nói trên, APIKey là Key ta nhận được khi đăng ký với OpenCellID, Area là tọa độ vùng ta cần lấy dữ liệu Cell-ID. OpenCellID sẽ trả về cho chúng ta dòng dữ liệu JSON. Sau đó, ta phải xử lý dòng dữ liệu JSON để lưu trữ Cell-ID trong cơ sở dữ liệu và biểu diễn nó trên bản đồ số.

Kết quả thể hiện dữ liệu Cell ID thu thập được như sau:

**Kết quả 1 (thể hiện trên bảng dữ liệu):*

- Vùng địa lý cần thu thập, tại Hà Nội, trong một hình chữ nhật giới hạn bởi các tọa độ:

20.99844829365592, 105.76860460265141

21.01401535951419, 105.75963510

- Nhà mạng: MCC 452 (Mobifone)

- Số lượng Cell Mobifone trong khu vực: 198.

** Kết quả 2 (thể hiện trên bản đồ số):*

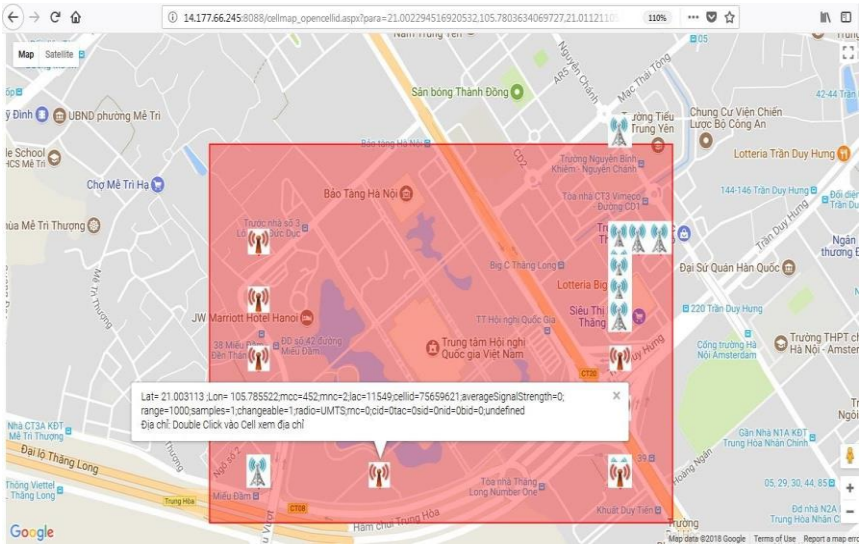
- Vùng chọn tại Hà Nội, giới hạn bởi các tọa độ:

+ 21.00229, 105.78036,

+ 21.01121, 105.79444.

Nhà mạng: MCC 452 (Mobifone).

Tổng số Cell-ID thu thập được: 99 (tại khu vực Trung tâm Hội nghị Quốc gia). Kết quả biểu diễn các Cell-ID của vùng chọn trên Google Maps như sau:



Hình 4. 1. Biểu diễn kết quả thu thập dữ liệu Cell-ID trên bản đồ số
(Trong đó các trạm gốc màu xanh là eNodeB 4G; Kích chuột vào trạm nào sẽ có số liệu Cell của trạm đó)

4.1.3. Thu thập từ dữ liệu Cell-ID từ nguồn của Google

4.1.3.1. Phương pháp

- Bước 1. Xác định vùng địa lý bất kỳ cần thu thập dữ liệu Cell-ID
- Bước 2. Request API tới http://www.google.com/glm/mmap
- Bước 3. Xử lý dòng dữ liệu trả về (response) bằng các phép toán dịch bit trái (left-shift operator) để nhận được danh sách các Cell trong khu vực với dữ liệu của nó.
- Bước 4. Sắp xếp dữ liệu trên bảng và biểu diễn dữ liệu trên bản đồ số.

Các bước 1-3 là yêu cầu dịch vụ của Google. Ví dụ bằng dòng lệnh đầu tiên như sau:

String url = "http://www.google.com/glm/mmap";

HttpWebRequest req = (HttpWebRequest)WebRequest.Create (new Uri(url));

4.1.3.2. Thực nghiệm và kết quả

Khi thực hiện lệnh Request trên với một tham số tương ứng, sau khi xử lý phản hồi bằng kỹ thuật dịch bit trái, ta nhận được tọa độ Cell-ID là (10.802742, 106.66104). Phần mềm sẽ xử lý và biểu diễn toạ độ này trên bản đồ số. Bản đồ thể hiện kết quả thu thập dữ liệu Cell-ID từ nguồn Google Maps sẽ được mô tả ở phần sau cùng với kết quả mô phỏng cải thiện độ chính xác định vị.

4.1.4. Nhận xét, đánh giá chung về thu thập dữ liệu Cell-ID từ nguồn mở

Việc lập trình modul phần mềm thu thập dữ liệu Cell-ID từ nguồn mở (từ nguồn OpenCellID và từ Google) cùng với xử lý kết quả thu thập được trên bảng dữ liệu hoặc bản đồ số đã được luận án thực hiện và ứng dụng thành công cho các thuật toán định vị liên quan đến dữ liệu Cell-ID. Định vị dựa trên Cell-ID là một trong những kỹ thuật định vị cơ bản theo nguyên lý kỹ thuật dựa trên mạng, ví dụ kỹ thuật định vị Cell-ID ToA, Cell-ID AoA đã được mô tả trong Chương 2.

Hai kết quả thực nghiệm nêu trên là một phần minh chứng cho giải pháp kỹ thuật định vị trên cơ sở kết hợp đa dạng nguồn dữ liệu: khi mà dữ liệu Cell-ID của mạng di động không có sẵn hoặc chưa đủ, chưa cập nhật (và thường là như vậy) hoặc khi mà muốn thu thập dữ liệu Cell-ID của nhà mạng nước ngoài, thì giải pháp kỹ thuật khả dụng là thu thập từ nguồn mở.

4.2. Cải thiện độ chính xác định vị

4.2.1. Phương pháp

Nội dung nghiên cứu giải pháp kỹ thuật cải thiện độ chính xác kỹ thuật định vị ToA, AoA đã được mô tả trong Chương 2 và công bố trong công trình số J2 trong Danh mục các công trình nghiên cứu liên quan đến đề tài luận án. Để cải thiện độ chính xác định vị ToA, AoA, luận án đã ứng dụng kết quả nghiên cứu và lập trình phần mềm để thực nghiệm. Một là, sử dụng thuật toán định vị có sẵn trên mạng để lập trình phần mềm định vị, thực hiện và lấy kết quả định vị thứ nhất. Hai là, sử dụng thuật toán đã được cải tiến, mở rộng lập trình phần mềm khác, thực hiện và lấy kết quả định vị thứ hai, sau đó tiến hành so sánh hai kết quả nêu trên.

Các bước thực nghiệm như sau:

- Bước 1. Thực hiện tính toán xác định vị trí của thiết bị di động theo thuật toán chưa được cải tiến, thể hiện trên bản đồ số.
- Bước 2. Thực hiện tính toán xác định vị trí của thiết bị di động theo thuật toán đã được cải tiến, thể hiện trên bản đồ số

(Mỗi bước 1 và 2 nêu trên được thực hiện hai lần bằng hai bộ dữ liệu đầu vào khác nhau để kiểm chứng)

- Bước 3. Ghi kết quả và so sánh.

4.2.2. Thực hiện và kết quả

4.2.2.1. Đặt vấn đề

Như đã trình bày, độ chính xác việc định vị thiết bị di động (MS/UE) phụ thuộc vào kết quả tính toán tọa độ điểm cắt nhau (Intersection Point) của các vòng tròn Cell-Id trong hệ tọa độ địa lý. Do đó, bản chất của việc cải thiện độ chính xác trong kỹ thuật định vị như đã trình bày chính là cải thiện độ chính xác của việc tính toán tọa độ điểm cắt nhau của các vòng tròn Cell-Id trong hệ tọa độ địa lý.

Sau đây, sẽ minh họa kết quả của việc xác định tọa độ điểm cắt nhau của các vòng tròn Cell-ID trong hệ tọa độ địa lý dựa trên hai thuật toán cải tiến và không cải tiến, chạy thử hai lần với hai bộ dữ liệu đầu vào.

4.2.2.2. Kết quả thực nghiệm

Để kiểm thử thuật toán cải tiến, chúng ta sẽ sử dụng chung dữ liệu đầu vào gồm tọa độ của 02 Cell-Id với tọa độ CellId-1, CellId-2 và bán kính lần lượt là *R1*, *R2*. Sau đó, tính toán tọa độ các điểm cắt nhau theo thuật toán cải tiến và không cải tiến rồi tạo bảng số liệu để so sánh.

- Thuật toán cải tiến: Thuật toán cải tiến đã nêu ở trên được lập trình và đưa lên tại ứng dụng Web "Hệ thống định vị - LTE-UMTS Posisioning System" được lập, chạy tại địa chỉ http://113.160.226.99:3392

- Thuật toán không cải tiến: Thuật toán không cải tiến đã nêu ở trên được lập trình bằng ngôn ngũ Rcode, việc thực thi Rcode sẽ chạy trên trang web https://www.mycompiler.io/new/r

Sử dụng 02 bộ dữ liệu để kiểm thử.

Kết quả thử bằng bộ dữ liệu 1:

CellId-1: 21.0093460083008; 105.78864288330; R1=75

CellId-2: 21.0095596313477; 105.78923034668; R2=80

Với bộ dữ liệu này, ứng dụng LTE-UMTS Posisioning System với thuật toán cải tiến cho kết quả 02 điểm cắt nhau như sau:

P(1): 21.01002048476; 105.788638280401

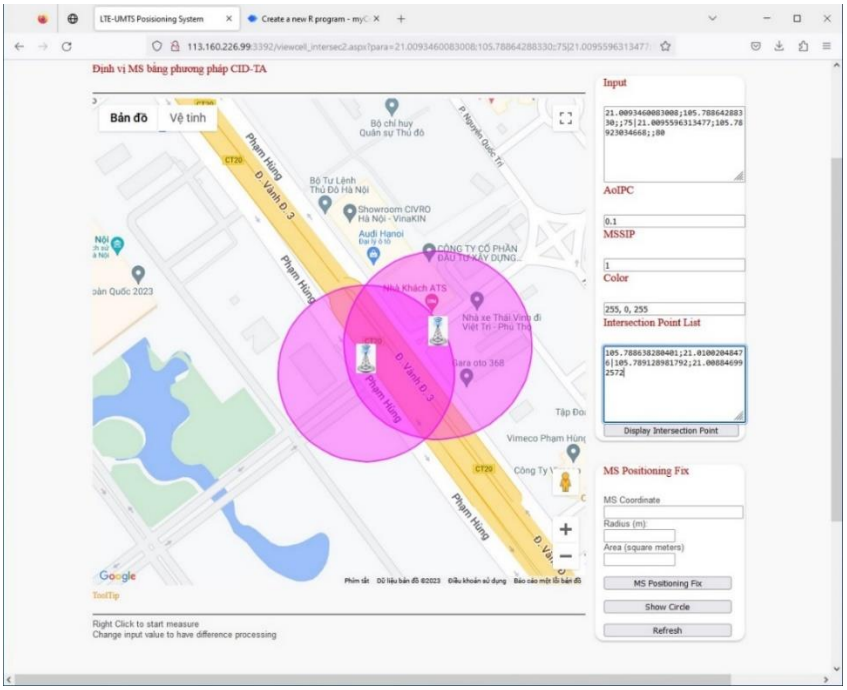
P(2): 21.008846992572; 105.789128981792

Ứng dụng Rcode cho kết quả các điểm cắt nhau như sau:

P(1): 21.0096903649321; 105.788750551508

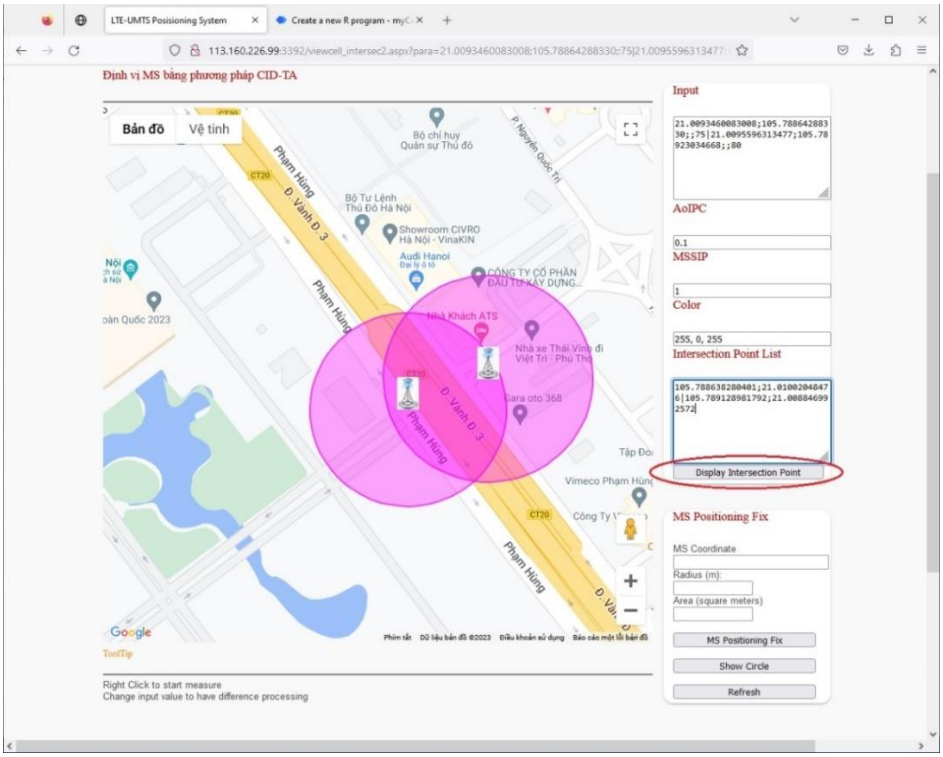
P(2): 21.0091603747375; 105.788971701646

Kết quả định vị:



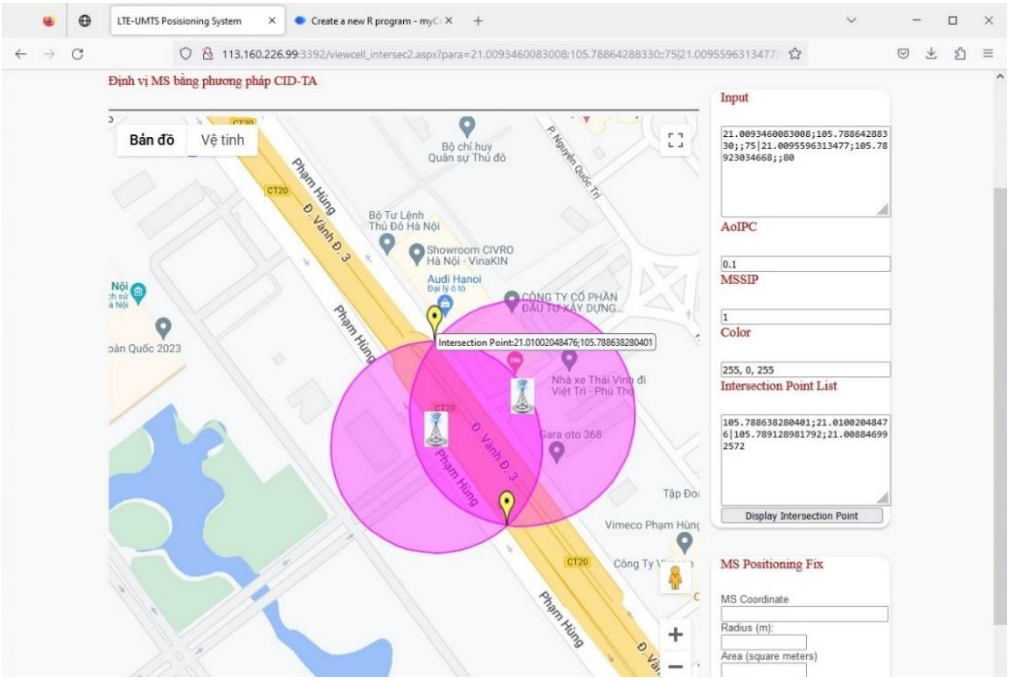
Hình 4. 2. Kết quả định vị trên bản đồ số của thuật toán cải tiến

Để xem sai số tọa độ điểm cắt nhau có hiển thị chính xác trên bản đồ không, click vào nút Display Intersection Point:



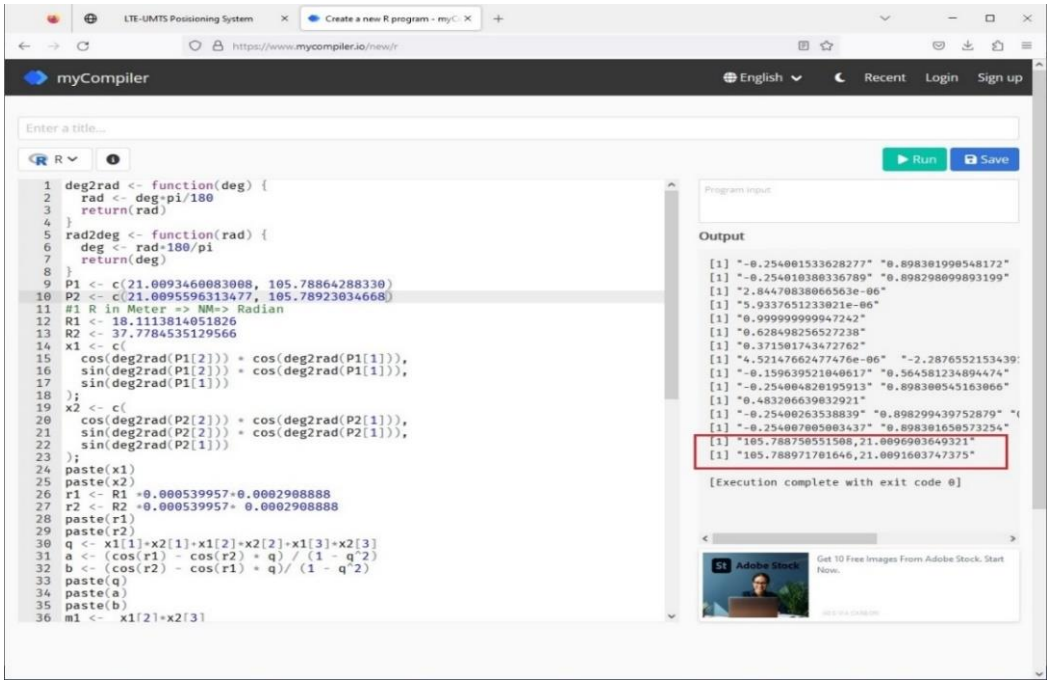
Hình 4. 3. Kiểm tra độ chính xác của thuật toán đã cải tiến

Nhìn trên bản đồ cho thấy, các điểm cắt nhau hiển thị chính xác trên bản đồ với sai số bằng 0 (m).

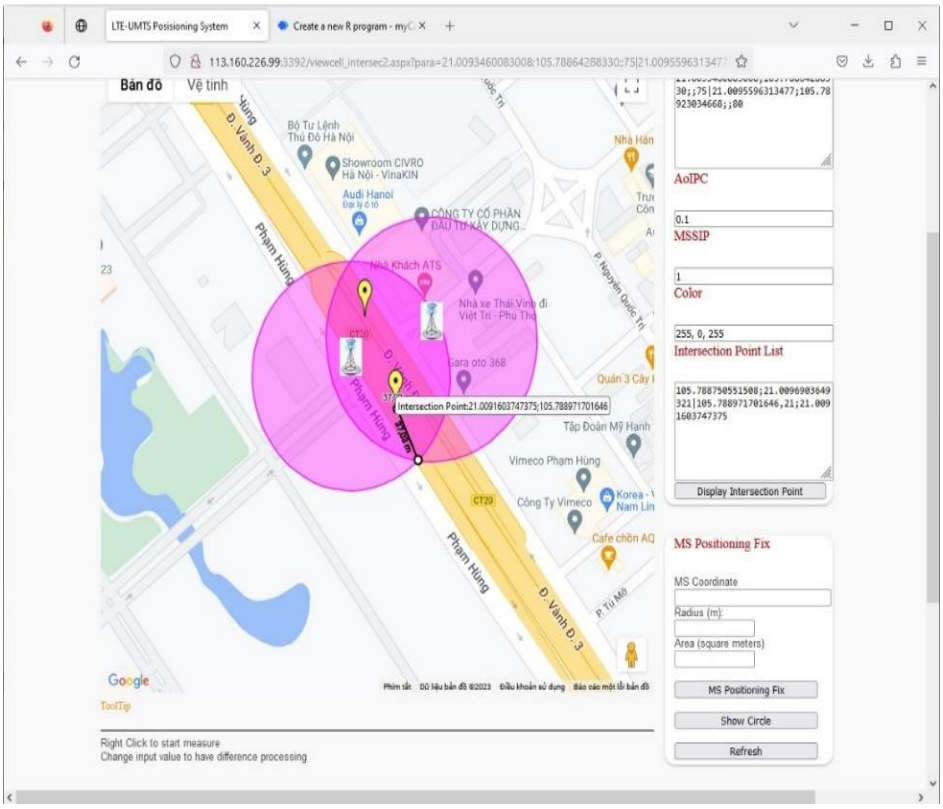


Hình 4. 4. Kết quả các điểm cắt nhau hiển thị chính xác trên bản đồ với sai số bằng 0 (m)

Kết quả định vị từ ứng dụng Rcode với thuật toán chưa cải tiến:



Hình 4. 5. Kết quả hiển thị các điểm cắt nhau không chính xác với sai số hơn 37(m)



Hình 4. 6. Bản đồ hiển thị các điểm cắt nhau không chính xác với sai số hơn 37(m)

Thử bằng Bộ dữ liệu 2:

CellId-1: 21.0095596313477; 105.78923034668; *R1*=75

CellId-2: 21.0093173980713; 105.789405822754; *R2*=80

Với bộ dữ liệu 2, thực hiện các bước tương tự như thử với bộ dữ liệu 1, ứng dụng LTE-UMTS Posisioning System đối với thuật toán đã cải tiến, cho kết quả 02 điểm cắt nhau với sai số 0 m và đối với chạy ứng dụng Rcode đối với thuật toán chưa cải tiến cho sai số là gần 55m. *(Việc thực hiện thử với hai bộ dữ liệu để đảm bảo tính tin cậy).*

Bảng sau đây sẽ so sánh kết quả kiểm thử cải tiến thuật toán định vị bằng hai bộ dữ liệu đầu vào nêu trên:

Bảng 4. 1. Bảng so sánh kết quả kiểm thử cải tiến thuật toán định vị

Dữ liệu đầu vào	**Tọa độ điểm cắt nhau**	
	Thuật toán cải tiến, mở rộng	Thuật toán không cải tiến
CellId-1: 21.0093460083008;	P(1) 21.01002048476;	P(1): 21.0095830407222; 105.789341798018

105.78864288330 R=75m ***CellId-2*:** 21.0095596313477; 105.78923034668 R=80m	105.788638280401 P(2) 21.008846992572 105.789128981792	P(2): 21.0094717893961; 105.789165571023
CellId-1: 21.0095596313477 105.78923034668 R=75 ***CellId-2:*** 21.0093173980713 105.789405822754 R=80	P(1) 21.009150156519; 105.788656205628 P(2) 21.009904512146; 105.789851276434	P(1): 21.0095830407222; 105.789341798018 P(2): 21.0094717893961; 105.789165571023
Sai số (m)	0	54,49

[J2; 23, 24, 26, 27, 28,29].

Bản đồ thể hiện kết quả định vị và bảng so sánh nêu trên cho thấy, với thuật toán cải tiến, tọa độ điểm cắt nhau của các vòng tròn CellID trong hệ tọa độ địa lý được xác định và tính toán chính xác 100% với sai số là 0 mét, trong khi, thuật toán không cải tiến có sai số 37 mét hoặc gần 55 mét. Sau khi tọa độ các điểm cắt nhau đã được tính chính xác, việc xác định tọa độ MS/UE trên tập các điểm cắt nhau cũng sẽ chính xác. Đó chính là ý nghĩa của việc cải tiến thuật toán xác định tọa độ điểm cắt nhau của các vòng tròn CellID cũng như là ý nghĩa của việc cải tiến độ chính xác của phương pháp định vị CellID-ToA, CellID-AoA như đã trình bày.

Trên cơ sở nghiên cứu và tìm ra thuật toán đúng đắn dựa trên một nguyên lý kỹ thuật định vị, luận án đã cải thiện được độ chính xác định vị trong các trường hợp khác nhau. Việc tính được vị trí và cải thiện được độ chính xác của nó chính là mục tiêu của quá trình định vị thiết bị di động.

4.2.3. Nhận xét, đánh giá

Kết quả thực nghiệm nêu trên cho thấy, độ chính xác định vị Cell-ID ToA và Cell-ID AoA trong hệ tọa độ địa lý đã được cải thiện sau khi cải tiến thuật toán định vị gốc. Kết quả thực nghiệm này đã minh chứng cho giải pháp kỹ thuật cải thiện độ chính xác kỹ thuật định vị ToA, AoA đã được trình bày trong Chương 2, minh chứng cho luận giải đề xuất giải pháp kỹ thuật định vị bằng hệ thống định vị lai ghép tiên

tiến với kết hợp nhiều kỹ thuật định vị khác nhau và sử dụng một số thuật toán định vị được cải tiến để nâng cao độ chính xác định vị.

4.3. Thực nghiệm giả lập trạm gốc thu thập tham số IMSI/IMEI

4.3.1. Kịch bản thực nghiệm

Luận án tiến hành thực nghiệm một số kỹ thuật liên quan, trong đó nghiên cứu thiết kế, chế tạo (bao gồm tích hợp linh kiện, thiết bị và lập trình phần mềm) thành công trạm gốc giả lập để thu thập tham số IMSI/IMEI, hỗ trợ phát hiện, định vị thiết bị di động. Trạm gốc giả lập được chế tạo bằng cách ứng dụng kỹ thuật vô tuyến định nghĩa bằng phần mềm (Software Defined Radio - SDR), lập trình phần mềm nhúng cho phép thiết lập thu phát sóng với các băng tần số phù hợp, có thể điều chỉnh công suất phát và thiết lập các tham số như một trạm gốc 3 băng tần của nhà mạng.

Trạm gốc giả lập trạm gốc có băng tần phù hợp với số liệu băng tần của các mạng di động có cung cấp 4G đã được khảo sát như bảng sau đây:

Bảng 4. 2. Băng tần di động của 3 nhà mạng chính

Nhà mạng	2G	3G	4G	Song công
Viettel	900/1800	2100	900/1800/2600	FDD
Vinaphone	900/1800	2100/900	1800	FDD
Mobifone	900/1800	2100	1800	FDD

Trên cơ sở giải pháp kỹ thuật giả lập trạm gốc thu thập tham số IMSI/IMEI tại Chương 3, ứng dụng kết quả của nhiệm vụ khoa học nêu trên, luận án đề xuất sử dụng trạm gốc giả lập đã chế tạo để thực nghiệm với các bước tiến hành như sau:

4.3.2. Các bước thực hiện và kết quả

4.3.2.1. Thu thập tham số IMSI/IMEI xác định vị trí tương đối của đối tượng

- Bước 1. Đo đạc thực tế, xác định các tham số cần thiết của mạng di động như vùng phủ, công suất, kênh tần số, MNC, Cell-LAC, Cell-ID. Sử dụng các thông số này để thiết lập tham số cho trạm giả khi tiến hành thực nghiệm.

- Bước 2. Triển khai trạm gốc giả lập 3 băng tần tại khu vực nghi ngờ đối tượng mang theo thiết bị di động 4G xuất hiện.

- Bước 3. Thực hiện phá sóng băng tần 3G.

- Bước 4. Điều chỉnh thông số trạm sao cho thiết bị di động 4G trong vùng đăng ký liên lạc qua modul trạm giả 4G.

(Lưu ý, công suất phát của trạm giả phải lớn hơn công suất phát của trạm thật mà điện thoại di động đối tượng đang đăng nhập; công suất phát của trạm giả càng cao thì khoảng cách từ trạm giả đến máy di động đối tượng cần thu tham số càng xa).

- Bước 5. Modul trạm giả 4G yêu cầu máy di động 4G thực hiện thủ tục cập nhật vị trí với tham số định danh tạm thời TMSI.

- Bước 6. Khi nhận được thủ tục cập nhật vị trí, modul trạm giả 4G trả lời điện thoại bằng bản tin từ chối cập nhật vị trí với nguyên nhân lỗi (trong 4G: EPS not allowed).

- Bước 7. Thiết bị di động sẽ không được phép truy cập vào các dịch vụ của mạng 4G tương ứng mà bắt buộc phải thực hiện lại thủ tục tìm kiếm tế bào mới trên mạng 2G, tìm thấy và đăng ký qua modul trạm giả 2G.

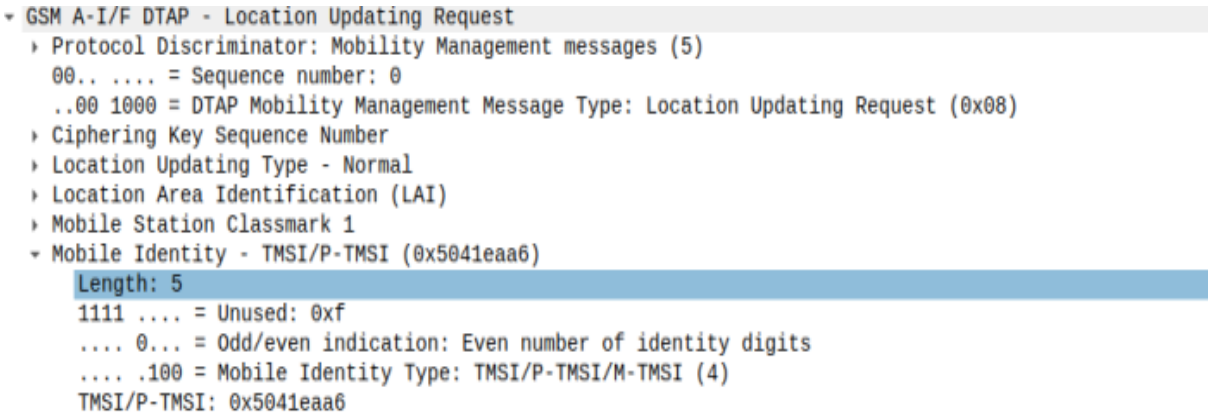
- Bước 8. Modul trạm giả 2G thực hiện thủ tục yêu cầu điện thoại xác thực thuê bao người dùng (theo thủ tục xác thực thuê bao người dùng 2G mà giải pháp kỹ thuật ở Chương 3 đã nêu) và trích xuất được tham số IMSI/IMEI.

Kết quả thực nghiệm thể hiện rằng đã thiết lập thành công trạm giả 2G và 4G, thực hiện phá sóng băng tần 3G và đã thu được tham số của điện thoại di động 4G như hình dưới đây:

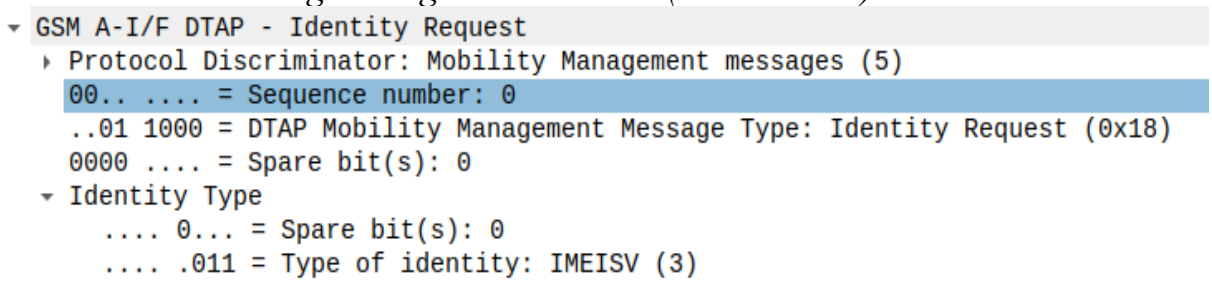
Trong mạng 4G:

*Hình 4. 7. Màn hình logfile của thực nghiệm giả lập trạm gốc 4G (với thể hiện tham số IMSI thu được là **452 02** 1111578159 - Vinaphone)*

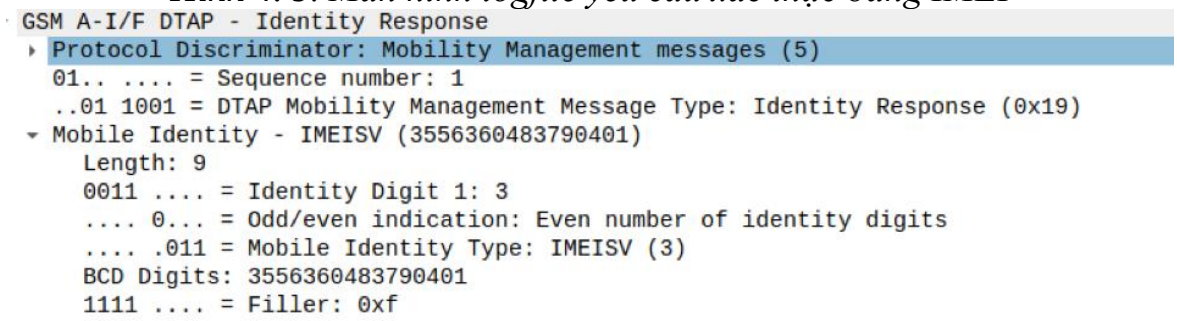
Trong mạng 2G:



Hình 4. 8. Màn hình logfile yêu cầu cập nhật vị trí của điện thoại vào mạng giả bằng tham số TMSI (0x5041eaa6)



Hình 4. 9. Màn hình logfile yêu cầu xác thực bằng IMEI



Hình 4. 10. Màn hình logfile điện thoại phản hồi xác thực bằng tham số IMEI

4.3.2.2. Đánh giá cự ly thu được tham số IMSI/IMEI

Như nguyên lý kỹ thuật giả lập trạm gốc đã phân tích, để có thể thu thập được tham số IMSI/IMEI của điện thoại mục tiêu, trạm gốc giả lập phải có các thông số giống như trạm thật và phát công suất đủ lớn để điện thoại mục tiêu đăng ký vào trạm. Theo lý thuyết tính toán đường truyền vô tuyến di động, phạm vi (cự ly) từ trạm gốc giả lập đến điện thoại mục tiêu mà sao cho mục tiêu có thể đăng ký vào trạm giả phụ thuộc vào nhiều tham số như: độ nhạy của máy thu tại trạm giả lập, môi trường sóng

vô tuyến tại khu vực, mật độ điện thoại tại khu vực, công suất phát của trạm giả lập v.v…Tuy nhiên, các tham số khác là ngẫu nhiên hoặc không điều chỉnh được, ví dụ độ nhạy máy thu là chỉ tiêu kỹ thuật của thiết bị thu SDR sẵn có, môi trường truyền sóng và mật độ máy di động là ngẫu nhiên.

Do vậy, muốn thay đổi cự ly, cơ bản là cần điều chỉnh công suất phát của trạm giả lập. Tất nhiên, cự ly này càng xa càng tốt, tức công suất phát càng cao càng tốt. Khi không thể ước lượng được khoảng cách có thể thì thường đặt công suất phát ở mức cao nhất và tiến lại càng gần khu vực nghi ngờ thì khả năng để mục tiêu đăng ký vào trạm càng cao. Triển khai thực nghiệm bằng cách thay đổi công suất phát của trạm gốc giả lập theo hai cách: đổi khối khuếch đại công suất từ 2W sang 10W hoặc điều chỉnh công suất phát của trạm gốc đang sử dụng bộ khuếch đại công suất 10W. Để kiểm chứng, luận án sử dụng màn hình điều khiển của trạm gốc giả lập để theo dõi thông số công suất thiết lập và dùng một máy phân tích phổ cầm tay để đo mức công suất phát, thay đổi tương ứng với cự ly từ trạm gốc giả lập đến máy di động mục tiêu mà đăng nhập được vào trạm gốc đó.

Kết quả thực nghiệm cho thấy trong một môi trường (địa điểm), nếu càng tăng công suất phát của trạm gốc giả lập thì cự ly mà điện thoại mục tiêu có thể đăng ký được vào mạng giả càng xa, tức phạm vi thu thập được tham số IMSI/IMEI và định hướng được mục tiêu của trạm gốc giả lập càng xa. Đồng thời, qua thực nghiệm cho thấy, với mạng di động thực tế và yêu cầu thu thập tham số ứng dụng cho công tác an ninh, công suất phát khả dụng của trạm giả lớn nhất là 10W. Theo logic đó, nếu giảm công suất phát của trạm giả mà vẫn thu thập được tham số IMSI/IMEI của điện thoại mục tiêu thì khu vực mà điện thoại đó xuất hiện càng hẹp (tức khoanh vùng định vị được một khu vực càng hẹp).

(Kết quả thực nghiệm đánh giá cự ly thu được tham số IMSI/IMEI sẽ được mô tả chung trong phần thực nghiệm tìm hướng ở mục 4.4).

4.3.3. Nhận xét, đánh giá

Bằng việc sử dụng một trạm gốc giả lập 3 băng tần với các bước như trên, luận án đã tiến hành thực nghiệm thu thập được tham số IMSI/IMEI của một thuê bao

(thiết bị) di động 4G. Từ đó, xác định rằng thiết bị di động, hay đối tượng, người cần tìm xuất hiện tại khu vực. Khu vực tương đối xác định được sự xuất hiện của điện thoại chính là phạm vi mà trạm gốc giả lập có thể thu chặn được tham số IMSI/IMEI của thiết bị di động. Khi đã xác định được khu vực tương đối, việc tìm kiếm vị trí đối tượng hay người mang theo thiết bị di động đó sẽ là khả thi.

4.4. Thực nghiệm tìm hướng, định vị thiết bị di động bằng trạm gốc giả lập

4.4.1. Nguyên lý kỹ thuật và kịch bản thực nghiệm

- Nguyên lý kỹ thuật

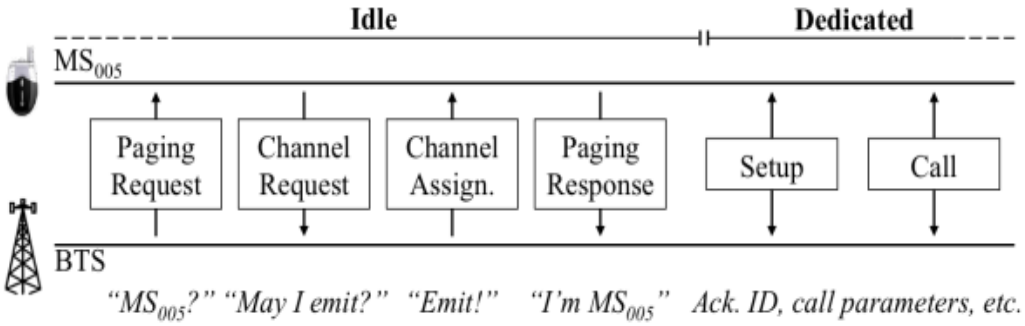
Về mặt kỹ thuật, có một số phương pháp định vị tầm gần vị trí điện thoại di động sau khi đã có vị trí tương đối. Trong đó, có thể sử dụng trạm gốc giả lập (đã thu thập được tham số IMSI/IMEI), liên tục yêu cầu điện thoại phát tín hiệu trên một kênh và dùng máy thu của trạm gốc giả lập đo cường độ tín hiệu đường lên. Khi đó, điện thoại di động cần tìm sẽ biến thành một nguồn phát tín hiệu như "đèn hiệu" dẫn đường. Thông qua giá trị đo được cường độ tín hiệu đường lên của điện thoại để ước tính hướng đến của nó so với máy thu. Tiến hành di chuyển dần trạm giả lập về hướng có tín hiệu mạnh nhất sẽ xác định được vị trí của điện thoại mục tiêu. Kỹ thuật này được gọi là tìm hướng (Direction Finding -DF). Việc tìm hướng có thể dùng chính trạm giả di chuyển dần đến nơi có cường độ tín hiệu đường lên thu được mạnh nhất như nêu trên hoặc dùng một máy thu định hướng cầm tay (Handheld DF Receiver) với hiển thị cường độ tín hiệu thu được từ đường lên của điện thoại mục tiêu bằng âm lượng hay LED chỉ thị mức.

Trở ngại lớn nhất chính là việc điện thoại không được thiết kế làm nguồn phát sóng liên tục trên một tần số cụ thể. Để làm việc này, trạm gốc giả lập cần thiết lập một mạng di động cục bộ (giả). Các băng tần 3G và 4G sẽ được gây nhiễu để toàn bộ điện thoại trong khu vực lựa chọn tế bào trên mạng cục bộ này và được xác thực bằng tham số IMSI/IMEI. Khi điện thoại hoạt động trong mạng cục bộ, thủ tục *Paging* được thực hiện thông qua thông số IMSI/IMEI để buộc điện thoại hoạt động ở chế độ kênh chuyên dụng và trở thành nguồn phát sóng cố định (đèn hiệu).

Sử dụng máy thu trong trạm gốc giả lập của mạng cục bộ và điều chỉnh để nghe cùng một kênh tần số đường lên của mạng dành riêng cho điện thoại di động mục tiêu. Thông qua cường độ tín hiệu cao tần (RF) của điện thoại trên đường lên để ước tính hướng đến của nó so với máy thu và sẽ xác định được khu vực vị trí nơi có cường độ tín hiệu thu được mạnh nhất.

- Thủ tục Paging

Trong mạng thông tin di động, để tiết kiệm năng lượng, MS/UE chuyển trạng thái sang chế độ *nhàn rỗi (idle)*; chúng chỉ giám sát RSSI của BTS/eNB lân cận phục vụ quá trình tái lựa chọn tế bào và tiếp tục theo dõi các tín hiệu *Paging* để sẵn sàng nhận cuộc gọi đến; trong chế độ này MS/UE sẽ không chủ động gửi bất kỳ thứ gì trên đường lên. Chế độ *kênh riêng (dedicated)* sẽ được kích hoạt khi điện thoại có cuộc gọi đi hoặc cuộc gọi đến. Để chuyển đổi từ chế độ *Nhàn rỗi* sang chế độ *Kênh riêng*, mạng sẽ gửi bản tin *Paging* trên một kênh chuyên dụng với tham số IMEI/IMSI/TMSI để tìm gọi điện thoại di động. Sơ đồ thủ tục Paging như sau:

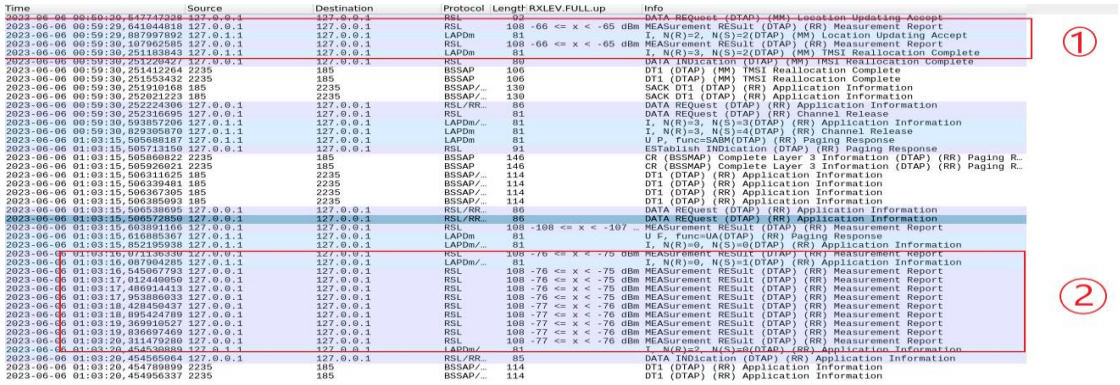


Hình 4. 11. Thủ tục paging thiết lập kênh riêng

Trong chế độ *kênh riêng*, cứ sau 480ms, MS/UE gửi một bản tin báo cáo đo lường (Measurement Report) trên kênh SACCH tới BSC của mạng, chứa các thông tin về cường độ tín hiệu MS/UE thu được của trạm BTS/eNB đang phục vụ và các trạm lân cận. Các thông tin này được BSC và MSC sử dụng cho quá trình chuyển giao. Tính năng này khiến MS/UE trở thành máy phát liên tục, và do vậy có thể theo dõi tín hiệu và xác định vị trí chính xác của nó theo phương pháp tìm hướng (DF). Phương pháp DF này thực hiện bằng cách di chuyển trạm gốc giả lập theo hướng tín hiệu thu được từ MS/UE ngày càng lớn hay sử dụng một thiết bị DF cầm tay dò tín hiệu và sẽ tiến dần được ngày càng gần MS/UE mục tiêu.

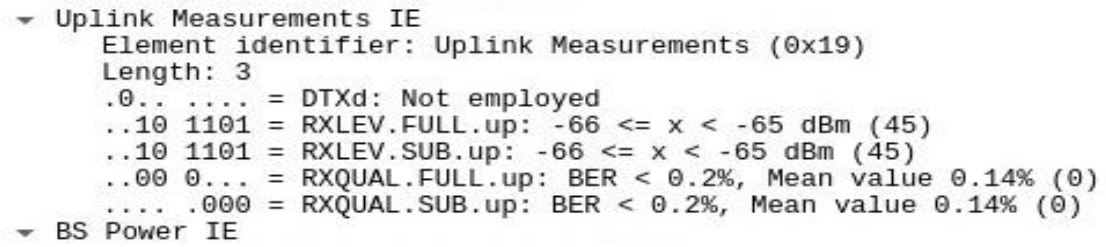
4.4.2. Kết quả

Tiến hành thực nghiệm, theo dõi giao diện Abis giữa Trạm gốc giả lập và BSC của mạng trong quá trình thực hiện *paging* điện thoại mục tiêu, ta xác định được các kết quả thể hiện như các ảnh chụp màn hình sau:



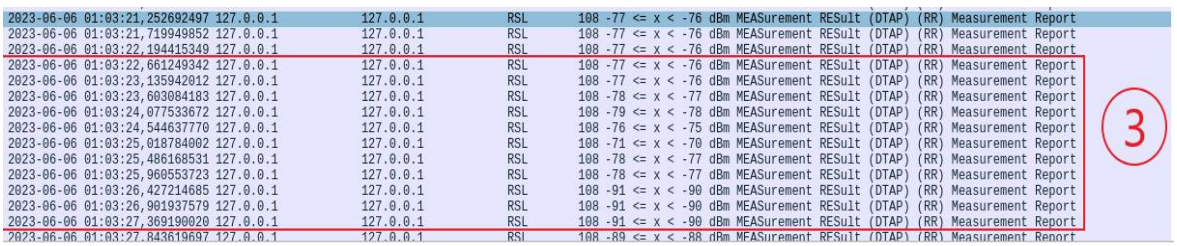
Hình 4. 12. Màn hình mô tả cường độ kết nối điện thoại mục tiêu đến trạm giả với khoảng cách gần hơn

Khuông đánh dấu số (1) là bản tin Meas-Rep khi MS/UE gửi khi thực hiện kết nối với mạng. Cột RXLEV.FULL.up thể hiện cường độ tín hiệu đường lên của MS/UE được đo bởi trạm giả.



Hình 4. 13. Màn hình logfile thể hiện cường độ tín hiệu đo được

Khuông đánh dấu số (2) thể hiện MS/UE liên tục gửi bản tin Meas-Rep khi thực hiện *paging*, trong trường hợp này vị trí của trạm giả không thay đổi so với vị trí MS/UE, vì vậy giá trị RXLEV.FULL.up dường như không đổi.



Hình 4. 14. Màn hình mô tả cường độ kết nối điện thoại mục tiêu đến trạm giả với khoảng cách xa hơn

Khuông đánh dấu số (3) cho thấy khi dịch chuyển vị trí trạm BTS/eNB giả lập ra xa so với vị trí của MS/UE, ta nhận được báo cáo đo lường công suất đường lên của điện thoại giảm hơn so với giá trị tại khuông đánh dấu số (2).

4.4.3. Nhận xét, đánh giá

Như tại khuông dánh dấu số (1), khi chưa thực hiện *paging,* điện thoại mục tiêu chỉ thực hiện các thủ tục đăng nhập vào mạng sau đó ngay lập tức chuyển về chế độ IDLE. Tại khuông đánh dấu số (2), sau khi thực hiện *paging,* điện thoại mục tiêu chuyển qua chế độ kênh riêng và liên tục gửi bản tin báo cáo đo lường trên kênh SACCH, do vậy điện thoại đã đủ điều kiện làm "đèn hiệu" vô tuyến, nên có thể định vị được theo giải pháp DF.

Kết quả thực nghiệm trên cho thấy khả năng tìm hướng, định vị tầm gần được một đối tượng chưa biết khi sử dụng trạm gốc giả lập. Kết quả này cũng minh chứng cho việc đánh giá cự ly thu thập được tham số IMSI/IMEI của trạm giả. Tại khuông đánh dấu (3), khi thay đổi khoảng cách xa điện thoại mục tiêu hơn vị trí mô tả tại khuông đánh dấu số (2), cường độ tín hiệu đường lên của MS/UE đã thay đổi giảm. Như vậy có thể kết luận cường độ tín hiêu thu phụ thuộc vào khoảng cách và ngược lại. Và nếu sử dụng giải pháp DF, thì khi trạm giả hoặc thiết bị DF cầm tay càng gần điện thoại mục tiêu hơn thì cường độ tín hiệu thu được càng lớn. [J3, 46-54].

4.5. Phân tích, đánh giá tổng hợp giải pháp kỹ thuật, mô hình hệ thống và kết quả một số thực nghiệm

Trên cơ sở các tồn tại, hạn chế và thách thức của vấn đề nghiên cứu, với các yêu cầu cụ thể của bài toán định vị thiết bị di động thế hệ thứ tư, luận án đã đề xuất giải pháp kỹ thuật sử dụng "hệ thống định vị lai ghép tiên tiến" trên cơ sở kết hợp đa dạng nguồn dữ liệu, cải tiến một số thuật toán định vị nhằm nâng cao hiệu quả định vị thiết bị di động; mô hình hệ thống định vị thiết bị di động trên cơ sở phân lớp định vị, bảo mật và trạm gốc giả lập ứng dụng cho công tác an ninh. Cùng với một số kết quả thực nghiệm đã trình bày ở trên cho thấy giải pháp kỹ thuật và mô hình hệ thống được đề xuất giải quyết được những vấn đề cơ bản còn tồn tại, hạn chế trong nghiên

cứu liên quan và đáp ứng được yêu cầu đặt ra. Bảng sau đây đánh giá tổng hợp một số vấn đề cơ bản như sau:

Bảng 4. 3. Đánh giá tổng hợp khả năng đáp ứng yêu cầu kỹ thuật

TT	Mô tả	Yêu cầu kỹ thuật	Khả năng đáp ứng	Phân tích, giải thích
1	Yêu cầu chung			
1.1	Xác định đối tượng định vị	Cụ thể như Bảng 2.1	Đáp ứng	Vì giải pháp định vị trên cơ sở kết hợp đa dạng nguồn dữ liệu và mô hình hệ thống sử dụng phân lớp định vị để xác định đối tượng
1.2	Định vị đối tượng	Cụ thể như Bảng 2.1	Đáp ứng	Vì giải pháp sử dụng hệ thống định vị lai ghép tiên tiến, cho phép áp dụng tổng hợp các nguyên lý kỹ thuật định vị, sử dụng nhiều nguồn dữ liệu khác nhau, cải tiến độ chính xác định vị; mô hình hệ thống kết hợp phân lớp định vị xác định chính xác đối tượng, áp dụng trạm gốc giả lập để hỗ trợ định vị nên đáp ứng được yêu cầu định vị đối tượng di động đa dạng với độ chính xác từ phạm vi rộng, tương đối, hẹp và chính xác. Các số liệu về cải thiện độ chính xác định vị kỹ thuật ToA, AoA; số liệu phân tích về bán kính khoanh vùng phạm vi hẹp và định hướng tiệm cần gần đối tượng khi tiến hành thực nghiệm đã minh chứng cho luận giải trên.
2.	Thu thập dữ liệu đầu vào của bài toán định vị	Cụ thể như Bảng 2.1	Đáp ứng	Giải pháp sử dụng đa dạng nguồn dữ liệu đầu vào; kết quả thực nghiệm thu thập dữ liệu Cell_ID từ nguồn mở minh chứng cho tính đáp ứng
3.	Thu thập dữ liệu tham chiếu của bài toán định vị	Cụ thể như Bảng 2.1	Đáp ứng	Giải pháp sử dụng đa dạng nguồn dữ liệu đầu vào; kết quả thực nghiệm thu thập dữ liệu Cell-ID từ nguồn mở minh chứng cho tính đáp ứng
4.	Đầu ra của bài toán định vị	Cụ thể như Bảng 2.1	Đáp ứng	Giải pháp kỹ thuật và mô hình hệ thống cùng một số kết quả thực nghiệm thu thập dữ liệu từ nguồn mở, cải thiện độ chính xác định vị (biểu diễn trên bản đồ số) và sử dụng trạm gốc giả lập thu thập

TT	Mô tả	Yêu cầu kỹ thuật	Khả năng đáp ứng	Phân tích, giải thích
				tham số IMSI/ IMEI hỗ trợ định vị chính xác minh chứng cho tính đáp ứng

4.6. Kết luận Chương 4

Chương 4 đã trình bày kịch bản, kết quả và đánh giá 4 thực nghiệm về thu thập dữ liệu Cell-ID từ nguồn mở; cải tiến thuật toán định vị Cell-ID ToA, Cell-ID AoA; sử dụng trạm giả lập để thu thập tham số IMSI/IMEI và tìm kiếm, định vị tầm gần thiết bị di động. Bảng phân tích tổng hợp 4.3 cùng các kết quả 4 thực nghiệm ở trên minh chứng giải pháp kỹ thuật và mô hình hệ thống định vị thiết bị di động ứng dụng cho công tác an ninh đã được trình bày trong Chương 2 và Chương 3.

KẾT LUẬN

Trong phạm vi nghiên cứu, đề tài luận án đã đề xuất giải pháp kỹ thuật lai ghép tiên tiến trên cơ sở kết hợp xử lý đa dạng nguồn dữ liệu đầu vào cùng các dữ liệu tham chiếu, cải thiện độ chính xác định vị nhằm nâng cao hiệu quả định vị thiết bị di động; xây dựng mô hình tổng thể hệ thống kỹ thuật định vị thiết bị di động trên cơ sở sử dụng phân lớp định vị, bảo mật chuyển giao kết quả định vị và giả lập trạm gốc để thu thập tham số IMSI/IMEI hỗ trợ phát hiện, định hướng, định vị tầm gần thiết bị di động. Đồng thời, luận án đã tiến hành các thực nghiệm cần thiết để minh chứng giải pháp kỹ thuật và mô hình hệ thống được đề xuất. Các giải pháp kỹ thuật được nghiên cứu, lựa chọn và mô hình hệ thống kỹ thuật được đề xuất đáp ứng yêu cầu định vị thiết bị di động thế hệ thứ tư và ứng dụng cho công tác an ninh.

Do vậy, có thể nhận thấy những đóng góp khoa học chính, tính mới của luận án như sau:

- Một là, đề xuất giải pháp kỹ thuật định vị trên cơ sở kết hợp đa dạng nguồn dữ liệu, cải tiến một số thuật toán định vị nhằm nâng cao hiệu quả định vị thiết bị di động.

Đây là giải pháp kỹ thuật có tính đặc thù để giải quyết các tồn tại, hạn chế và thách thức của bài toán định vị thiết bị di động thế hệ thứ tư, hoạt động được trên nền mạng 4G nói chung và mạng 4G Việt Nam nói riêng.

- Hai là, đề xuất mô hình hệ thống định vị thiết bị di động trên cơ sở sử dụng phân lớp định vị, bảo mật và trạm gốc giả lập ứng dụng cho công tác an ninh.

Đây là một mô hình tổng thể trên cơ sở kỹ thuật định vị lai ghép tiên tiến đã chọn, có đa dạng đầu vào dữ liệu, sử dụng phân lớp định vị, bảo mật và trạm gốc giả lập để thực hiện các chức năng. Hệ thống có tính mở và tính mới để giải quyết các yêu cầu phức tạp định vị thiết bị di động thế hệ thứ tư của công tác an ninh.

Luận án cũng đã tiến hành một số thực nghiệm trong môi trường mạng di động Việt Nam, minh chứng giải pháp kỹ thuật và mô hình hệ thống định vị đã đề xuất, thể hiện khả năng ứng dụng thực tiễn cao của giải pháp cho công tác an ninh.

HƯỚNG PHÁT TRIỂN CỦA LUẬN ÁN

Để có thể ứng dụng được kết quả của đề tài luận án vào công tác nghiên cứu khoa học, kỹ thuật định vị di động mới nói chung và công tác an ninh nói riêng, luận án đề xuất hướng nghiên cứu, phát triển tiếp theo là:

- Nghiên cứu sâu hơn một số giải pháp kỹ thuật: khoa học dữ liệu, giải pháp nền tảng dữ liệu mở; ứng dụng trí tuệ nhân tạo (AI), học máy (ML) cho bài toán xử lý dữ liệu định vị.
- Nghiên cứu mở rộng giải pháp kỹ thuật và mô hình hệ thống cho định vị thiết bị di động 5G trên môi trường mạng thực tế sẽ được triển khai trong thời gian tới.

DANH MỤC CÁC CÔNG TRÌNH KHOA HỌC ĐÃ CÔNG BỐ

[C1] Ho Van Canh, Le Danh Cuong, Le Hai Trieu, Nguyen Hong Thuy, Tran Huu Binh, Tran Dinh Tuan, Nguyen Huy Hung, “Criteria for Assessing the Safety of Sercured Information”, Proceedings of the Second Vietnam International Applied Mathematics Conference (VIAMC 2017), TP Hồ Chí Minh.

[C2] Nguyễn Hồng Thủy, Hồ Văn Canh, Lê Danh Cường, Lê Nhật Thăng, "Giải bài toán phân lớp không có giám sát liên quan tới điều khiển chuyển vùng", Kỷ yếu Hội nghị Quốc gia lần thứ XXI về Điện tử, Truyền thông và Công nghệ thông tin (REV - ECIT 2018), Hà Nội.

[C3] Nguyễn Hồng Thủy, Hồ Văn Canh, Lê Nhật Thăng, Nguyễn Quốc Thắng, Trần Đình Tuấn, “Một phương pháp giải bài toán chia sẻ bí mật", Kỷ yếu Hội nghị Quốc gia lần thứ XXII về Điện tử, Truyền thông và Công nghệ thông tin (REV - ECIT 2019), Hà Nội.

[C4] Nguyễn Văn Chung, Nguyễn Hồng Thủy, “Đề xuất một thuật toán giấu tin mật", Hội thảo Quốc gia “Ứng dụng Công nghệ cao vào thực tiễn - 60 năm phát triển Viện Khoa học và Công nghệ quân sự”, Hà Nội, 2020.

[J1] Nguyễn Hồng Thủy, Hồ Văn Canh, Lê Nhật Thăng, "Một phương pháp định vị đối tượng dựa trên phân lớp có giám sát", Tạp chí Nghiên cứu Khoa học và Công nghệ quân sự, Hà Nội, 2018.

[J2] Nguyễn Hồng Thuỷ, Trần Cao Hiên, “Nghiên cứu cải thiện độ chính xác trong kỹ thuật định vị TOA và AOA”, Tạp chí Khoa học Công nghệ Thông tin và Truyền thông, Số 4 (CS.01), Hà Nội, 2022.

[J3] Nguyễn Hồng Thuỷ, Lê Duy Trường, “Giải pháp kỹ thuật giả lập trạm gốc thu thập tham số IMSI/IMEI, hỗ trợ phát hiện, định vị thiết bị di động” Tạp chí Khoa học Giáo dục Kỹ thuật - Hậu cần, Bộ Công an, Số 33/2023.

DANH MỤC TÀI LIỆU THAM KHẢO

Các công trình nghiên cứu trong nước

[1] Tổng cục Thống kê, "Thông cáo Báo chí Về tình hình kinh tế - xã hội Quí IV và năm 2022", kỳ tham chiếu: 2022, ngày đăng: 29/12/2022.

[2] Thủ tướng Chính phủ, Quyết định số 411/QĐ-TTg ngày 31/3/2022, "Phê duyệt Chiến lược quốc gia phát triển kinh tế số và xã hội số đến năm 2025, tầm nhìn đến năm 2030".

[3] Lê Danh Cường, "Phát triển phương pháp định vị và giám sát thuê bao GSM đặc thù qua giao diện vô tuyến", Luận án Tiến sĩ kỹ thuật, Học viện Công nghệ Bưu chính Viễn thông, Hà Nội, 2018.

[4] Vũ Trung Kiên, "Nghiên cứu, phát triển kỹ thuật định vị trong nhà sử dụng tín hiệu Wifi", Luận án Tiến sĩ kỹ thuật; Viện Ứng dụng công nghệ; Hà Nội 2019.

[5] Bộ Thông tin và Truyền thông, "Khung tham chiếu ICT phát triển hệ thống đô thị thông minh, phiên bản 1.0", ban hành kèm theo Quyết định số 829/QĐ-BTTTT ngày 31/5/2019 của Bộ trưởng Bộ Thông tin và Truyền thông.

[6] QCVN 110:2017/BTTTT, "Qui chuẩn kỹ thuật quốc gia về thiết bị trạm gốc thông tin di động E-UTRAN, phần truy nhập vô tuyến", Hà Nội, 2017.

[7] Phạm Anh Phương, Quách Hải Thọ, "Một số giải pháp quản lý dữ liệu tham gia phân lớp trong mô hình học bán giám sát" - Kỷ yếu Hội nghị quốc gia lần thứ X về nghiên cứu cơ bản và ứng dụng dụng công nghệ thông tin (FAIR), Đà Nẵng 17 - 18 /8/2017; DOI: 10.15625/vap. 2017 - 00059.

[8] Hồ Văn Canh, Lê Hải Triều, "Vai trò của toán học trong phân tích mật mã" - Sách chuyên khảo: NXB Công an nhân dân, Tháng 5/ 2021.

[9] Lương Viết Nguyên, Hồ Văn Canh, Trịnh Nhật Tiến, "Solving language recognition problem" (IJCSIS): International Journal of Computer Science and Information Security, Vol.xxx, No.xxx. 2010.

[10] Lê Ngọc Hưng, Nguyễn Xuân Quỳnh, "Nhận dạng và phân lớp các yếu tố ảnh hưởng tới điều khiển chuyển vùng", Kỷ yếu Hội nghị quốc gia lần thứ X về

nghiên cứu cơ bản và ứng dụng công nghệ thông tin (FAIR), Đà Nẵng 17-18/8/2017. DOI: 10.15625/vap. 2017 - 00085.

[11] Hồ Văn Canh, Lê Hải Triều, "Kỹ thuật nhận dạng bản rõ" - Tạp chí Khoa học Giáo dục Kỹ thuật, hậu cần - Bộ Công an; số 7 - 2016; ISSN: 2354 - 1008.

[12] Hồ Văn Canh, Nguyễn Viết Thế, "*Phần 1 Nhập môn: Phân tích thông tin có bảo mật*'', Nhà xuất bản Hà Nội T&T – 2010.

Các công trình nghiên cứu nước ngoai (Tiếng Anh)

[13] Alfred J. Menezes, Paul C. Van Oorschot; Scott A. Vanstone: "Handbook of Applied Cryptography" - CRC Press: Boca Raton - New York - London - Tokyo, 1999.

[14] C. Rao's: "Linear Statistical Theory and its applications". Moscow, 1968

[15] R.E. Blahut "Digital Transmission of Information" Reading, MA: Addison - Wesley, 1990.

[16] Stephen B. Wicker "Error control systems for digital communication and storage" Prentice Hall - New Jersey, 1999.

[17] T. Baritaud, M. Campana, P. Chauvaud, and H. Gilbert "On the security of the permuted kernel identification scheme - Advances in Cryptology" - CRYPTO' 93 (LNCS 740), 305 - 311, 1993.

[18]T. Cover and J. Thomas (1991): "Elements of Information Theory" New York: Wiley Inter-Science, 1991.

[19] Sidharth Gopal, Y. Yang, Konstation Salomation Jaime Carbonell: "Statistical learning for File - Type Indentification". By: Digital Intelligence and Investigation Directorate in the Software Engineering Institute, CMU 2012.

[20]Luc Devroye, László Györfi and Gábor Lugosi "A probabilistic Theory of Pattern Recognition" Springer - Verlag New York, NY 10027, USA New York, Inc. 1996.

[21] K. Kirchhoff, S. Parandekar, "Multi - stream statisticcal n-gram modeling with application to automatic Language Identification", in European Speech Communication Association (EUROSPEECH), pp. 803-806 (2001).

[22] Ravi Ganesan and Alan T. Sherman, “Statistical Techniques for Language Recognition: An Introduction and Guide for Cryptanalysts”, CRYPTOLOGIA October 1993, Vol. XVII, No. 4.

[23] Ayad M. H. Khalel, “Position Location Techniques in Wireless Communication Systems”, MEE10: 67 Electrical Engineering Emphasis on Telecommunications October 2010.

[24] Andreas Schmidt-Dannert, “Positioning Technologies and Mechanisms for Mobile Devices”, Seminar Master Module SNET2 TU-Berlin, 2012.

[25] FCC, “911 and E911 Services, standards and requirements”, “In October 1999, the Wireless Communications and Public Safety Act of 1999” (911 Act), USA.

[26] Christopher Drane, Malcolm Macnaughtan, and Craig Scott, “Positioning GSM Telephones”, IEEE Communications Magazine, April 1998.

[27] Brian O’Keefe, “Finding Location with Time of Arrival and Time Difference of Arrival Techniques”, ECE Senior Capstone Project 2017 Tech Notes.

[28] Omar Waleed Abdulwahhab, Mobile Position Estimation based on Three Angles of Arrival using an Interpolative Neural Network, International Journal of Computer Applications (0975 – 8887) Volume 100– No.7, August 2014.

[29] Yao Zhang, Zhongliang Deng and Yuhui Gao, “Angle of Arrival Passive Location Algorithm Based on Proximal Policy Optimization”, Electronics 2019, 8, 1558; doi:10.3390/ electronics8121558.

[30] ETSI TS 123 171 V3.10.0 (2003-06), Technical Specification, “Universal Mobile Telecommunications System (UMTS); Location Services (LCS); Functional description; Stage 2 (UMTS) (3GPP TS 23.171 version 3.10.0 Release 1999).

[31] Mrs. Ashwini B, Dr. Usha J, “Location Based Services - Positioning Techniques and its Applications”, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 1, January 2014.

[32] M.F.M.Mahyuddin, A.A.M.Isa, M.S.I.M.Zin, Afifah Maheran A.H, Z.Manap and M.K.Ismail, “Overview of Positioning Techniques for LTE Technology”, e-ISSN: 2289-8131 Vol. 9 No. 2-13.

[33] Rafael Saraiva Campos, “Evolution of Positioning Techniques in Cellular Networks, from 2G to 4G”, Hindawi Wireless Communications and Mobile Computing Volume 2017.

[34] Albert Montilla Bravo, Jose lgnacio Moreno, lgnacio Soto, “ADVANCED POSITIONING AND LOCATION BASED SERVICES IN 4G MOBILE-IP RADIO ACCESS NETWORKS”, 0-7803-8523-3/04/$20.00 02004 IEEE.

[35] Mike Thorpe, Ewald Zelmer, “LTE Location Based Services - Technology Introduction” Rohde & Schwarz, September, 2015.

[36] Erisson White Paper, “Positioning With LTE”, September 2011.

[37] Zhang Bo, Du Yuanfeng, and Yang Dongkai, “The Impact of New Features on Positioning Technology in LTE-A System”, Hindawi Pbulising Corporation, Volume 2015.

[38] Pedro J. Fernández, José Santa, and Antonio F. Skarmeta, “Hybrid Positioning for Smart Spaces: Proposal and Evaluation”, Appl. Sci. 2020, 10, 4083; doi:10.3390/app1012408.

[39] Kamiar Radnosrati, Carsten Fritsche, Fredrik Gunnarsson, Fredrik Gustafsson and Gustaf Hendeby, “Localization in 3GPP LTE Based on One RTT and One TDOA Observation”, IEEE Transactions on Vehicular Technology, 69(3), 3399-3411.

[40] Jeongyeup Paek, Ramesh Govindan, Kyu-Han Kim, Jatinder P. Singh, “Energy-Efficient Positioning for Smartphones using Cell-ID Sequence Matching”

[41] Heng Zhang, Zhichao Zhang , Shunqing Zhang , Shugong Xu and Shan Cao, “Fingerprint-based Localization using Commercial LTE Signals: A Field-Trial Study”, Shanghai University, Shanghai, 200444, China, July, 2019.

[42] Suhui Jeong, Halim Lee, “RSS-based LTE Base Station Localization Using Single Receiver in Environment with Unknown Path-Loss Exponent”, Yonsei University Incheon, Korea, 2020.

[43] SPIRENT, “An Overview of LTE Positioning”, White Paper, SPIRENT Americas 1-800, 2018.

[44] Jose A. del Peral-Rosado, Jose A. Lopez-Salcedo, Gonzalo Seco-Granados, Francesca Zanier, and Massimo Crisci, “Analysis of positioning capabilities of 3GPP LTE”, Universitat Autonoma de Barcelona (UAB), Spain, European Space Agency (ESA), The Netherlands, September, 2012.

[45] Juan Luis Bejarano-Luque * , Matías Toril , Mariano Fernández-Navarro , Luis Roberto Jiménez and Salvador Luna-Ramírez, “Statistical Model for Mobile User Positioning Based on Social Information”, CEI Andalucía TECH, 29071 Málaga, Spain, 2021.

[46] ETSI TS 132 421 V9.1.0 (2010-2014), UMTS/ LTE Subscriber and Equipment Trace; Trace Concepts and Requirements.

[47] 3GPP TS 25.331: RRC Protocol Specification

[48] 3GPP TS 25.304: UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected mode

[49] 3GPP TS 21.133: 3G Security; Security Threats and Requirements.

[50] 3GPP TS 24.301 V10.12.0 (2013-12), 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 10)

[51] O. Dunkelman, N. Keller, and A. Shamir,“A practical-time attack on the A5/3 cryptosystem used in third generation GSM telephony”, 2010.[1] A. Dubey, D. Vohra, K. Vachhani and A. Rao, "Demonstration of vulnerabilities in GSM security with USRP B200 and open-source penetration tools," 2016 22nd Asia-Pacific Conference on Communications (APCC), Yogyakarta, Indonesia, 2016, pp. 496-501, doi: 10.1109/APCC.2016.7581461.

[52] Řezník, Tomáš & Horáková, Bronislava & Szturc, Roman. (2013). Advanced methods of cell phone localization for crisis and emergency management applications. International Journal of Digital Earth. 8. 1-14. 10.1080/17538947.2013.860197.

[53] Arapinis, Myrto & Mancini, Loretta & Ritter, Eike & Ryan, Mark. (2017). Analysis of privacy in mobile telephony systems. International Journal of Information Security. 16. 10.1007/s10207-016-0338-9.

[54] S. Zorn, M. Gardill, R. Rose, A. Goetz, R. Weigel and A. Koelpin, "A smart jamming system for UMTS/WCDMA cellular phone networks for search and rescue applications," 2012 IEEE/MTT-S International Microwave Symposium Digest, Montreal, QC, Canada, 2012, pp. 1-3, doi: 10.1109/MWSYM.2012.6257769.

[55] TA9 Big Data Analysis Flatform for Cyber Intelligence Solution (Rayzone Group, Israel).

[56] Geo Matrix Mobile Phone System Positioning (Rayzone Group, Israel).

[57] Systems for Signalling Control in 2G/3G/4G network (Shinetech, Finland/ UAE).

[58] Hybrid Location (Skyhock, Qualcomm, USA).