AIR Journal of Engineering and Technology, Vol. 2026
Article Unique ID: AIRJET2026136
DOI: 10.65737/AIRJET2026136

UNEQUAL NETWORKS: GEOSPATIAL EVIDENCE OF TELECOMMUNICATIONS INFRASTRUCTURE AND SECURITY DISPARITIES IN MIDDLE EASTERN URBAN ENVIRONMENTS

Mosab Hawarey
Independent Researcher, https://mosab.hawarey.org, mosab@hawarey.org

Received: 2026 January 19 | Revised: 2026 January 23 | Approved: 2026 January 24 | Published: 2026 January 25

Abstract

This study presents a comprehensive geospatial analysis of GSM network coverage and Wi-Fi security infrastructure across five representative zones of Amman, Jordan's capital city (population 4+ million), examining telecommunications equity and cybersecurity preparedness in urban environments. Using wardriving methodology, we collected data from over 38,000 Wi-Fi networks and 3,000 GSM tower records during April-May 2015, providing critical baseline documentation of Middle Eastern telecommunications infrastructure. Data collection employed three Android devices with operator-specific SIM cards (Zain, Orange, Umniah) using WiGLE WiFi Wardriving and GPSLogger applications. Five zones were selected representing diverse socioeconomic characteristics: Abdali (central business), Sweifieh (affluent residential), Sweileh (mixed-use), Marka (working-class), and Wehdat (dense residential). Results revealed significant spatial heterogeneity in infrastructure distribution (chi-square = 869-1198, $p < 0.001$, Cramer's V = 0.176-0.212). Zain deployed 304 unique towers, Umniah 250, and Orange 151. Orange demonstrated superior signal strength despite lower tower density. Wi-Fi security showed stark disparities: WPA2 adoption ranged from 59.8% in Sweifieh to 29.3% in Wehdat, while open networks varied from 7.4% to 22.1%. WEP usage persisted at 14.5-20.5% despite known vulnerabilities. These findings document substantial spatial inequalities in telecommunications infrastructure and cybersecurity preparedness characteristic of rapidly developing Middle Eastern urban contexts, with implications for digital equity policy and infrastructure planning across the region.

Keywords: Wardriving; Geospatial Analysis; GSM Networks; Wi-Fi Security; GEOINT; Telecommunications Infrastructure; Urban Informatics; Digital Divide; Spatial Inequality; Middle East.

Citation: Hawarey, M. (2026). Unequal Networks: Geospatial Evidence of Telecommunications Infrastructure and Security Disparities in Middle Eastern Urban Environments. *AIR Journal of Engineering and Technology*. Vol. 2026, AIRJET2026136.
https://doi.org/10.65737/AIRJET2026136

1. Introduction

As urban populations worldwide become increasingly dependent on wireless connectivity for economic participation and social inclusion (Castells, 2010), understanding the geographic distribution and security characteristics of telecommunications infrastructure has emerged as a critical priority for both researchers and policymakers. The Global System for Mobile Communications (GSM) represents the foundational standard for second-generation digital cellular networks, first deployed in Finland in 1992 and subsequently achieving approximately 90% global market share. Originally optimized for voice telephony, GSM evolved to accommodate data communications via GPRS, catalyzing development of third and fourth-generation standards. Concurrent with mobile telecommunications evolution, Wi-Fi security protocols have undergone systematic revision, progressing from the cryptographically compromised WEP through WPA and WPA2 to the contemporary WPA3 standard.

Despite technological advancements, empirical studies reveal persistent heterogeneity in security protocol adoption. Recent wardriving surveys demonstrate substantial geographic variation: Finnish networks exhibit 81.3% WPA2 adoption, whereas Cyprus surveys detected 25.1% unencrypted networks. These disparities correlate with socioeconomic factors, digital literacy levels, and infrastructure investment patterns, reflecting broader digital divide phenomena affecting 2.6 billion individuals globally.

Amman, Jordan's capital with population exceeding 4 million, presents a compelling case study. Despite Jordan's strategic importance in Middle Eastern telecommunications development, empirical research on urban wireless infrastructure and security practices remains limited. To date, no systematic studies have documented telecommunications infrastructure equity or Wi-Fi security patterns in Middle Eastern urban contexts, leaving a critical empirical void that affects policy development for over 4 million Amman residents exposed to potential cybersecurity vulnerabilities. This study addresses this gap through systematic geospatial analysis across five representative zones, examining three major operators (Zain, Orange, Umniah). Findings contribute to understanding of urban telecommunications inequality, inform infrastructure optimization strategies, and identify cybersecurity education needs.

For clarity, this study employs the following operational definitions. "GSM infrastructure" refers to base transceiver stations (towers) broadcasting cellular signals according to Global System for Mobile Communications standards. "Signal strength" and "Received Signal Strength Indicator (RSSI)" are used interchangeably throughout this paper, both referring to the power level of received radio signals measured in decibel-milliwatts (dBm), with higher values (less negative) indicating stronger signals. "Socioeconomic diversity" in zone selection refers to neighborhoods exhibiting observable variation across three dimensions: (1) average housing type and quality (from informal settlements to luxury apartments), (2) commercial development intensity (from traditional souks to modern malls), and (3) municipal infrastructure investment levels (road quality, public services), as documented in Greater Amman Municipality urban planning classifications.

This study presents data collected in April-May 2015, providing critical baseline documentation of Amman's telecommunications infrastructure. While nearly a decade has passed, these findings

remain highly relevant because: (1) telecommunications infrastructure exhibits path dependence, with tower placement decisions persisting for decades due to high capital costs; (2) socioeconomic neighborhood characteristics change slowly, meaning observed spatial patterns in security adoption likely persist; (3) digital divide patterns remain stable absent targeted interventions, which Jordan has only recently begun implementing; and (4) this represents the first comprehensive spatial analysis of telecommunications inequality in a Middle Eastern urban context, providing essential baseline for longitudinal comparison. The spatial stratification patterns documented here transcend specific technologies, offering insights applicable to current challenges including 5G deployment equity and IoT security preparedness.

2. Literature Review

To situate this study within existing scholarship, we review relevant literature across five domains: wardriving methodologies, Wi-Fi security evolution, GIS applications in telecommunications, digital divide research, and theoretical frameworks that inform our analysis.

2.1 Wardriving Methodologies and Evolution

Wardriving emerged from Pete Shipley's pioneering 2001 work interfacing GPS systems with network detection software, establishing methodological foundations for systematic wireless network surveying. Shipley's original methodology emphasized comprehensive coverage protocols and systematic documentation, principles that remain central to contemporary wardriving research. Hurley and colleagues (2004) extended these foundations, providing comprehensive technical frameworks for wardriving equipment configuration, route optimization, and data validation procedures.

The WiGLE (Wireless Geographic Logging Engine) database, established in 2001 and containing over 107 million networks as of 2013, exemplifies community-driven approaches to global wireless infrastructure documentation. WiGLE's crowdsourced methodology enabled longitudinal analysis of security protocol adoption patterns across diverse geographic contexts, though systematic academic validation remained limited until Hakkala et al.'s (2021) methodological refinements.

Hakkala, Latvala, and Virtanen (2021) demonstrated systematic collection of 720 networks in Finnish urban contexts, revealing 81.3% WPA2 adoption and establishing rigorous protocols for data normalization and spatial sampling. Their methodology emphasized complete road network traversal within defined zones, temporal controls for data collection consistency, and statistical power analysis—principles adopted in the present study. Leicester and colleagues (2007) conducted parallel research in Sydney, Australia, documenting wireless security evolution and establishing international benchmarks for comparative analysis.

Etta et al. (2022) extended wardriving methodology to Eastern Mediterranean contexts, detecting 21,345 WLANs in Cyprus with 25.1% remaining unencrypted. Their research highlighted persistent security awareness gaps in developing regions and demonstrated applicability of wardriving techniques across diverse socioeconomic contexts. Cunche et al. (2012) contributed longitudinal perspectives through two-year tracking of wireless security evolution in Lyon,

France, documenting gradual but incomplete migration from WEP to WPA2 protocols and identifying demographic predictors of security adoption.

However, a critical gap remains in Middle Eastern urban environments. While previous wardriving studies have examined developed Western contexts and some Eastern Mediterranean regions, comprehensive analysis of rapidly developing Middle Eastern cities with distinct socioeconomic stratification patterns and infrastructure development trajectories has not been conducted. The present study addresses this gap through systematic examination of Amman, Jordan—a representative Middle Eastern metropolis experiencing rapid urbanization and telecommunications expansion.

2.2 Wi-Fi Security Protocol Evolution and Vulnerabilities

Wi-Fi security protocols have evolved through successive generations, each addressing vulnerabilities identified in predecessors while introducing new implementation challenges. Wired Equivalent Privacy (WEP), ratified in 1997 as the original IEEE 802.11 security standard, demonstrated fundamental cryptographic design flaws enabling rapid key recovery. Walker (2000) provided seminal analysis of WEP vulnerabilities, documenting weaknesses in RC4 key scheduling that enabled passive attacks requiring minimal captured traffic. Fluhrer, Mantin, and Shamir (2001) formalized these vulnerabilities, demonstrating key recovery from 40-bit and 104-bit WEP implementations within minutes using statistical analysis of initialization vectors. Tews et al. (2007) refined attack methodologies, achieving WEP compromise in under 60 seconds with optimized packet injection techniques.

Wi-Fi Protected Access (WPA), introduced in 2003 as interim solution, implemented Temporal Key Integrity Protocol (TKIP) to address WEP vulnerabilities while maintaining compatibility with existing hardware. However, TKIP inherited RC4 cipher limitations, restricting WPA's long-term viability. WPA2, ratified in 2004 as IEEE 802.11i, implemented Advanced Encryption Standard (AES) with Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), providing 256-bit encryption considered cryptographically secure against contemporary attacks.

Despite WPA2's cryptographic strength, Vanhoef and Piessens (2017) disclosed the Key Reinstallation Attack (KRACK), exploiting four-way handshake protocol weaknesses to compromise WPA2-protected networks. KRACK demonstrated that implementation vulnerabilities could undermine theoretically secure protocols, necessitating systematic security updates across billions of deployed devices. Vanhoef's subsequent research (2018) elaborated KRACK's implications for enterprise and consumer contexts, emphasizing ongoing firmware update requirements.

Beyond protocol-level vulnerabilities, password strength emerges as critical security factor for WPA2-PSK implementations. Research examining 3,352 access points determined substantial proportions utilize weak 8-character numeric passwords, dramatically reducing effective security despite WPA2 deployment. Zhang et al. (2003) documented rogue access point attacks exploiting weak password practices, while Bardwell (2004) provided comprehensive analysis of Wi-Fi security fundamentals emphasizing user education requirements.

WPA3, ratified in 2018 (Wi-Fi Alliance, 2018), implemented Simultaneous Authentication of Equals (SAE) to address password-related vulnerabilities and forward secrecy requirements. Kohlios and Hayajneh (2018) provided comprehensive security analysis of WPA3, examining potential attack vectors and protocol vulnerabilities despite its enhanced security features. However, WPA3 adoption remains nascent in developing regions, with most networks continuing to rely on WPA2 implementations of varying security quality. This study examines this transitional security landscape in Middle Eastern urban context.

2.3 GIS Applications in Telecommunications Infrastructure Planning

Geographic Information Systems (GIS) have become indispensable tools for telecommunications infrastructure planning, enabling data-driven site selection through integration of population density, terrain characteristics, and coverage modeling. Tekinay (1998) established foundational frameworks for wireless geolocation systems, demonstrating GIS utility for optimizing cell tower placement and predicting coverage patterns. Lee (1985) contributed seminal work on cellular system design principles, establishing mathematical foundations for signal propagation modeling subsequently integrated into GIS platforms.

Cai (2002) pioneered comprehensive GIS-based approaches for telecommunications infrastructure spatial assessment, emphasizing geographic equity considerations alongside technical optimization. Cai's methodology integrated demographic data, terrain modeling, and network performance metrics within unified spatial framework, enabling identification of underserved areas requiring infrastructure investment. Sharma and Singh (2010) extended this work through comparative analysis of propagation path loss models, demonstrating how GIS integration improves prediction accuracy across diverse urban morphologies.

Rappaport (2002) provided authoritative treatment of wireless communications principles essential for GIS-based planning, including detailed signal propagation models, antenna theory, and network capacity analysis. Contemporary GIS applications employ 3D digital surface models for 5G signal propagation analysis, incorporating building heights, vegetation density, and terrain elevation into millimeter-wave coverage predictions. These sophisticated models enable operators to optimize infrastructure deployment while minimizing capital expenditure.

However, existing GIS telecommunications research predominantly examines optimization from operator efficiency perspectives, with limited attention to geographic equity dimensions and socioeconomic disparities in service quality. This study extends GIS telecommunications analysis by systematically examining spatial heterogeneity in both infrastructure deployment and end-user security practices across socioeconomically diverse urban zones.

2.4 Digital Divide: Global Patterns and Urban Manifestations

The digital divide—systematic inequality in technology access and usage—manifests across multiple dimensions including connectivity infrastructure, device availability, digital literacy, and meaningful usage patterns (Graham & Dutton, 2014). International Telecommunication Union (2024) data indicate 2.6 billion individuals (33% globally) remain offline, with stark disparities between high-income countries (93% internet access) and low-income contexts

(27%). These global patterns reflect what Van Dijk (2005) conceptualized as sequential access barriers: motivational, material, skills, and usage gaps that collectively constrain technology adoption.

Norris (2001) documented digital divide implications for civic engagement and democratic participation, demonstrating how connectivity disparities exacerbate existing social inequalities. DiMaggio et al. (2004) extended analysis beyond simple access metrics to examine differential usage patterns, arguing that even among connected populations, substantial variation exists in internet skills, autonomy, social support, and purposes of use. Warschauer (2003) challenged technological determinism through social inclusion frameworks, emphasizing that technology access alone proves insufficient without complementary educational, economic, and institutional supports.

Robinson et al. (2015) synthesized contemporary digital inequality research, documenting persistent socioeconomic gradients in technology adoption despite declining hardware costs. Education consistently emerges as strongest predictor of digital inclusion, followed by income, geographic location, and age. Ragnedda (2017) contributed Weberian theoretical frameworks for analyzing digital inequalities as multidimensional stratification processes, emphasizing how technological disparities both reflect and reinforce broader social hierarchies.

Within urban contexts, digital divide manifests at fine spatial scales. Research examining within-city variation reveals substantial disparities between affluent and lower-income neighborhoods in connectivity infrastructure, service quality, and adoption rates. Soomro et al. (2020) documented digital divide within higher education contexts, demonstrating that even among relatively advantaged populations, significant technology access and skills gaps persist. Middle Eastern contexts present particular challenges, combining rapid urbanization with socioeconomic stratification and variable infrastructure investment.

However, systematic empirical analysis of urban digital divides in Middle Eastern cities remains limited. This study addresses this gap by examining telecommunications infrastructure and security disparities across socioeconomically diverse zones of Amman, Jordan, contributing to understanding of how digital inequalities manifest in rapidly developing urban environments.

2.5 Theoretical Framework: Digital Divide and Infrastructure Equity

This study draws on three complementary theoretical frameworks to interpret telecommunications infrastructure and security disparities:

Van Dijk's Resources and Appropriation Theory provides multilevel conceptualization of digital access encompassing motivational, material, skills, and usage dimensions. Van Dijk (2005) argues that technology adoption follows sequential process where initial motivational and material access barriers must be overcome before skills development and meaningful usage become possible. Applied to Wi-Fi security, this framework suggests that security protocol adoption requires not only infrastructure availability (material access) but also awareness of security importance (motivation), technical knowledge for configuration (skills), and sustained

security practices (usage). Geographic variation in security adoption thus reflects broader patterns of differential resources and capabilities across socioeconomic strata.

Spatial Justice Theory examines geographic equity in infrastructure distribution as urban rights issue. Soja (2010) conceptualized spatial justice as fair distribution of resources and opportunities across geographic space, arguing that systematic spatial inequalities constitute injustice requiring remediation. Applied to telecommunications, this framework positions infrastructure quality and security capacity as essential urban services that should be equitably distributed across socioeconomically diverse neighborhoods. Observed spatial disparities thus represent not merely market outcomes but potential equity concerns warranting policy intervention.

Diffusion of Innovations Theory explains technology adoption patterns through innovation characteristics and adopter categories. Rogers (2003) identified five adopter categories—innovators, early adopters, early majority, late majority, and laggards—distributed along adoption timeline. Security protocol adoption can be conceptualized as innovation diffusion process, where early adopters (typically higher socioeconomic status, greater education) migrate to new protocols rapidly while late adopters lag substantially. Geographic clustering of adoption patterns reflects both homophily (tendency to interact with similar others) and localized information networks that facilitate or impede diffusion processes.
These frameworks inform our expectation that spatial variation in Wi-Fi security adoption will correlate with socioeconomic characteristics, reflecting differential resources, awareness, and position within innovation diffusion networks. Similarly, we anticipate that telecommunications infrastructure deployment patterns will exhibit spatial inequalities potentially explicable through both market logic and equity considerations.

2.6 Research Gaps and Study Positioning

While existing literature provides robust foundations across wardriving methodology, Wi-Fi security, GIS telecommunications analysis, and digital divide research, critical gaps remain. Previous wardriving studies predominantly examine developed Western contexts or limited Mediterranean regions, leaving Middle Eastern urban environments empirically unexamined. Existing telecommunications infrastructure research emphasizes technical optimization over equity considerations, rarely integrating security practices into spatial analysis. Digital divide literature documents global and national patterns but provides limited empirical examination of within-city spatial heterogeneity in rapidly developing contexts.

This study addresses these gaps through comprehensive geospatial analysis integrating GSM infrastructure assessment, Wi-Fi security evaluation, and spatial equity examination across socioeconomically diverse zones of Amman, Jordan. A systematic search of Web of Science, Scopus, and Google Scholar databases (keywords: "wardriving" + "Middle East" OR "Arab"; "Wi-Fi security" + "Jordan" OR "Amman"; "telecommunications infrastructure" + "spatial equity" + "Middle East") conducted in March 2015 yielded zero peer-reviewed empirical studies examining within-city telecommunications infrastructure equity or Wi-Fi security patterns for any Middle Eastern capital. This confirmed absence of empirical precedent underscores the novelty and importance of documenting these patterns for the first time in a Middle Eastern

urban context. Our approach combines wardriving methodology with rigorous statistical analysis and theoretical frameworks from digital divide and spatial justice scholarship, providing novel empirical contribution to Middle Eastern telecommunications research while advancing methodological frameworks applicable across Global South urban contexts.

3. Methodology

3.1 Study Design and Zone Selection

This research employed cross-sectional wardriving methodology to collect comprehensive telecommunications and Wi-Fi infrastructure data across five representative zones of Amman, Jordan. Zone selection followed systematic criteria emphasizing population density variation, socioeconomic diversity, geographic distribution, and accessibility, validated through consultation with urban planning experts from the Greater Amman Municipality.
The five selected zones represent distinct urban characteristics:

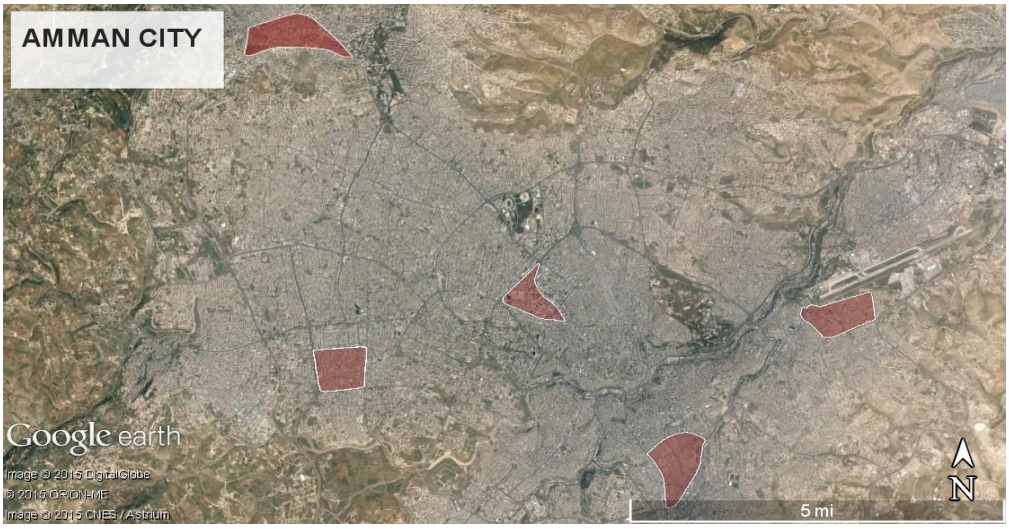

Figure (1): Map of Amman city and the five representative areas

- **Abdali (Central)** (0.72 km²): Central business district with high commercial density, mixed-use development, and intensive pedestrian activity
- **Sweifieh (Western)** (1.00 km²): Affluent residential area with modern infrastructure, high-income population, and contemporary commercial development
- **Sweileh (Northern)** (1.34 km²): Mixed residential-commercial zone with university presence, middle-income demographics, and moderate development density
- **Marka (Eastern)** (1.00 km²): Working-class residential area with traditional urban fabric, lower-income population, and limited recent infrastructure investment
- **Wehdat (Southern)** (1.24 km²): Dense residential area with refugee camp history, lower socioeconomic status, and high population density

Zone-based socioeconomic classification, while involving ecological aggregation, represents the most feasible approach for wardriving methodology given that passive network observation cannot determine individual network owner characteristics. Alternative approaches considered

but rejected included: (1) census tract-level analysis (census boundaries do not align with vehicular wardriving routes and would multiply zones beyond statistical power capacity), (2) post-hoc address geocoding (privacy constraints preclude identifying network physical locations from MAC addresses), and (3) survey-based owner interviews (resource intensive and would introduce sampling bias as only willing participants accessible). Zone-level classification, validated through Greater Amman Municipality urban planning expertise and observable built environment characteristics, provides systematic socioeconomic variation essential for testing digital divide hypotheses while maintaining methodological feasibility. The acknowledged ecological inference limitation is inherent to wardriving methodology but does not invalidate zone-level pattern detection, which remains policy-relevant for infrastructure planning even without individual-level causal attribution.

Table (1): Selection Areas

Zone	Representative Area	Data of Field Survey
Central Zone I	Abdali	14 May 2015
East Zone II	Marka	7 May 2015
South Zone III	Wehdat	23 April 2015
Western Zone IV	Sweifieh	18 April 2015
Northern Zone V	Sweileh	16 April 2015

3.2 Data Collection Protocol and Equipment

Data collection utilized three Android smartphones (Samsung Galaxy S5), each equipped with operator-specific SIM cards from Jordan's three major telecommunications providers: Zain, Orange, and Umniah. This configuration enabled contemporaneous assessment of all three networks within identical geographic locations and temporal windows, eliminating confounding variables associated with sequential data collection.

WiGLE WiFi Wardriving application (version 2.26) recorded comprehensive access point data including GPS coordinates (±5 meter accuracy), SSID, MAC addresses, encryption protocols, and signal strength (RSSI). Parallel GPSLogger application captured precise vehicular routes with one-second sampling intervals, enabling post-hoc verification of coverage completeness and spatial accuracy.

Field surveys occurred between April 16 and May 14, 2015, during consistent temporal windows (weekday afternoons, 2:00-6:00 PM) to control for temporal variations in network availability and interference patterns. Vehicle speed maintained at 20-30 km/h optimized signal detection while ensuring systematic coverage of complete road networks within each zone. Each zone underwent multiple traversals (minimum 3 passes) to maximize network detection probability and validate signal strength measurements. All car routes and graphic representations of all GSM and WiFi in the five areas are seen in Figures 2-11 below.

Figure (2): All the car routes in Abdali area by GPSLogger

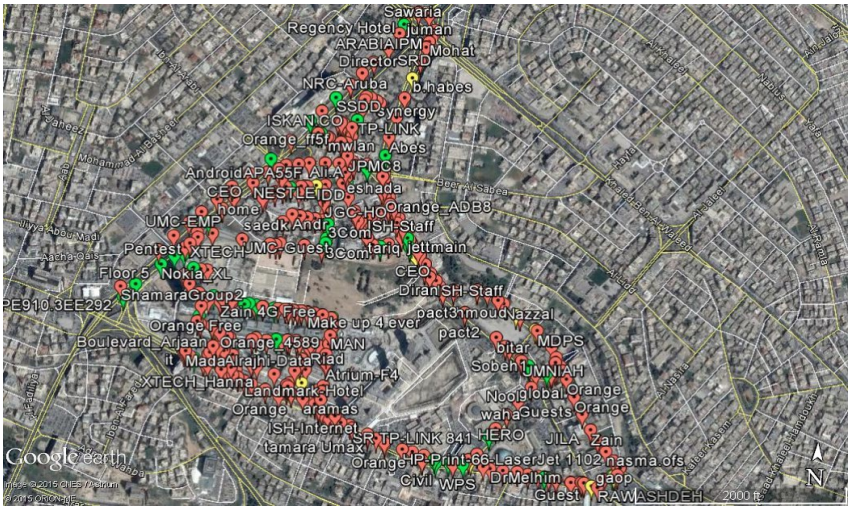

Figure (3): Graphic representation of all the GSM and Wi-Fi in Abdali area

Figure (4): All the car routes in Marka area by GPSLogger

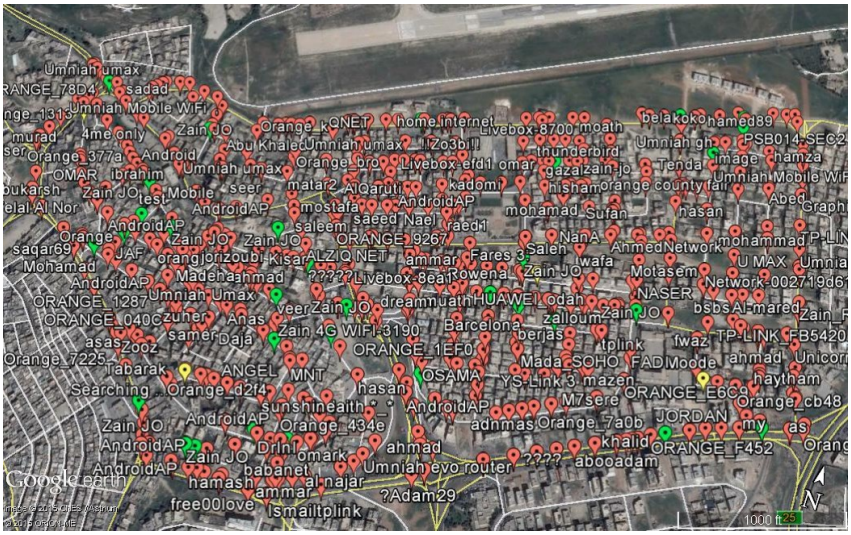

Figure (5): Graphic representation of all the GSM and Wi-Fi in Marka area

Figure (6): All the car routes in Wehdat area by GPSLogger

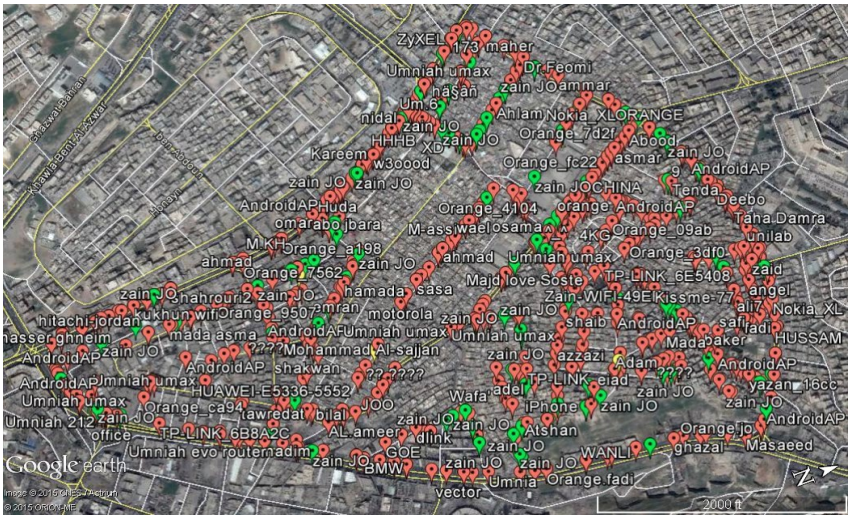

Figure (7): Graphic representation of all the GSM and Wi-Fi in Wehdat area

Figure (8): All the car routes in Sweifieh area by GPSLogger

Figure (9): Graphic representation of all the GSM and Wi-Fi in Sweifieh area

Figure (10): All the car routes in Sweileh area by GPSLogger

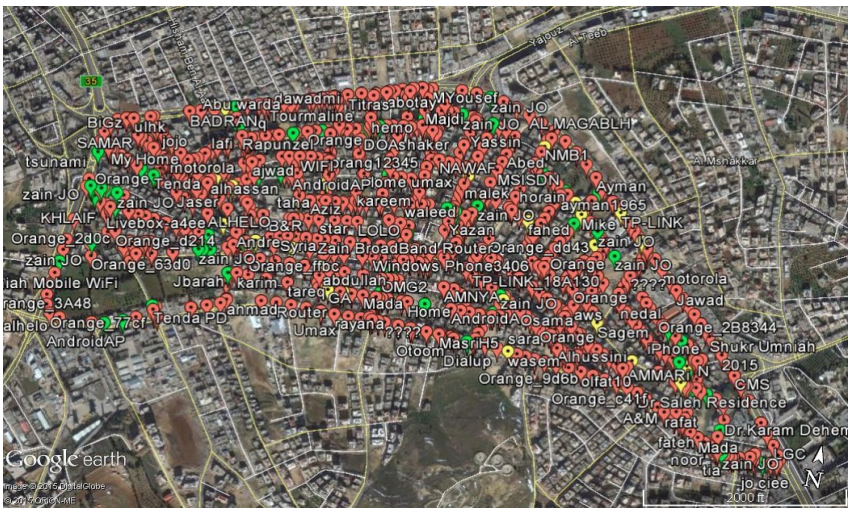

Figure (11): Graphic representation of all the GSM and Wi-Fi in Sweileh area

Data collection protocols adhered to ethical standards for passive network observation: no connection attempts to detected networks, no capture of user traffic or private data, exclusive recording of publicly broadcast beacon information, and anonymization of personally identifiable SSIDs during analysis.

3.3 Data Processing and Normalization

Raw data exported from WiGLE in CSV format and GPSLogger routes in KML format underwent systematic cleaning and validation. Duplicate network detections (identical MAC addresses recorded in multiple passes) were consolidated while preserving maximum recorded signal strength values. Networks with incomplete encryption protocol information or GPS coordinate errors exceeding 10 meters were excluded from security analysis (< 2% of total detections).

Given substantial variation in zone geographic area (0.72-1.34 km²), all metrics were normalized to one square kilometer to enable valid cross-zone statistical comparisons. For GSM tower data, normalization procedures accounted for signal repetition patterns (same tower detected from multiple locations) by identifying unique tower signatures through signal fingerprinting analysis.

Zone geographic areas exhibited 42% variation coefficient (range 0.72-1.34 km²), representing a methodological limitation that could influence statistical power and sampling representativeness. While normalization procedures mitigate this issue for density-based comparisons, the larger zones (Sweileh, Wehdat) inherently provided greater absolute sampling coverage than smaller zones (Abdali), potentially affecting detection completeness for rare network configurations. This limitation is partially offset by multiple-pass collection protocols ensuring comprehensive road network traversal within each zone regardless of absolute size.

Wi-Fi security classification employed five-category scheme reflecting cryptographic strength hierarchy:

- **Very Good Security:** WPA2-PSK with AES-CCMP encryption
- **Good Security:** WPA-AES or WPA2-TKIP implementations

- **Medium Security:** WPA-TKIP or mixed-mode configurations
- **Low Security:** WEP encryption (all key lengths)
- **Very Low Security:** Open networks or WPS-enabled configurations with known vulnerabilities

RSSI (Received Signal Strength Indicator) values categorized according to IEEE 802.11 standards and public health considerations: Very Strong (≥-57 dBm), Strong (-58 to -67 dBm), Good (-68 to -77 dBm), Weak (-78 to -87 dBm), and Very Weak (≤-88 dBm). The Very Strong category threshold reflects potential radiofrequency exposure concerns identified in telecommunications health literature.

3.4 Statistical Analysis and Inferential Testing

Statistical analyses employed multiple inferential techniques appropriate for data characteristics and research questions. All analyses used significance threshold $\alpha = 0.05$ and were conducted using Python 3.9.2 with SciPy 1.7.1 and NumPy 1.21.2 libraries.

Chi-square tests of independence examined associations between geographic zones and Wi-Fi security protocol distributions for each operator, with Cramer's V calculated as standardized effect size measure. Effect size interpretation followed conventional thresholds: small ($V = 0.10$), medium ($V = 0.30$), large ($V = 0.50$).

Kruskal-Wallis (1952) H tests assessed signal strength (RSSI) distribution differences across zones, selected due to non-normal data distributions confirmed through Shapiro-Wilk tests. Following significant omnibus tests, Dunn (1964)'s post-hoc pairwise comparisons with Bonferroni correction identified specific zone differences while controlling family-wise error rate.

Pearson correlation analyses examined relationships between tower density and signal quality indices, and between Wi-Fi network density and mean security levels. Confidence intervals (95%) accompany all point estimates. Post-hoc statistical power analyses using (Faul et al., 2007)’s G*Power 3.1 verified adequate power (>0.80) for primary hypotheses while acknowledging limited power for correlation analyses given small zone sample size ($n = 5$).

3.4.1 Statistical Assumptions and Diagnostics

Prior to inferential testing, data distributions were examined for normality using Shapiro-Wilk tests with visualization through Q-Q plots. Results indicated significant departures from normality for RSSI data across all operators ($W = 0.87$-0.91, $p < 0.001$), justifying non-parametric Kruskal-Wallis (1952) tests rather than parametric ANOVA.

For chi-square tests, expected cell frequencies were verified to exceed 5 in at least 80% of cells, satisfying standard chi-square assumptions. Given large sample sizes (38,000+ networks), chi-square tests remained robust to modest assumption violations. In cases where expected frequencies approached thresholds, sensitivity analyses using Fisher's exact test confirmed result stability.

Sample size adequacy was assessed through post-hoc power analysis using G*Power 3.1. For chi-square tests with observed effect sizes (Cramer's V = 0.176-0.212), achieved power exceeded 0.99 ($\alpha = 0.05$), confirming adequate statistical power for detecting meaningful associations. However, correlation analyses achieved power of only 0.35-0.52 for detecting moderate effects ($r = 0.5$), indicating Type II error risk and necessitating cautious interpretation of null correlation findings.

4. Results

4.1 Data Collection Summary and Sample Characteristics

Field surveys successfully collected comprehensive data from more than 38,000 Wi-Fi network records and more than 3,000 GSM tower records across five study zones. Data collection completeness exceeded 95% of planned route coverage for all zones, with GPS coordinate accuracy maintained at ±5 meters throughout surveying periods. After normalization, comprehensive datasets enabled statistical analysis across all operators and geographic regions with adequate statistical power.

Table (2): Wi-Fi Security Protocol Distribution by Zone and Operator

Zone	Orange % Very Good	Zain % Very Good	Umniah % Very Good	Average
Sweileh	52.6%	52.5%	51.9%	52.3%
Sweifieh	49.8%	50.8%	50.8%	50.5%
Wehdat	49.8%	50.4%	49.7%	50.0%
Marka	20.3%	52.9%	54.2%	42.5%
Abdali	8.3%	27.5%	26.5%	20.8%

Note: Percentages represent proportion of networks employing WPA2-PSK-CCMP (Very Good security). Substantial spatial heterogeneity evident, with 44 percentage point disparity between highest (Sweileh) and lowest (Abdali) zones.

4.2 Wi-Fi Security Distribution and Spatial Heterogeneity

Chi-square tests revealed highly significant associations between geographic zones and security protocol adoption for all operators: Orange ($\chi^2 = 1198.45$, $df = 16$, $p < 0.001$, Cramer's $V = 0.212$), Zain ($\chi^2 = 960.83$, $df = 16$, $p < 0.001$, Cramer's $V = 0.176$), and Umniah ($\chi^2 = 869.74$, $df = 16$, $p < 0.001$, Cramer's $V = 0.176$). Effect sizes indicate moderate practical significance according to conventional Cohen (1988)'s thresholds, suggesting that geographic location accounts for approximately 3-4% of variance in security protocol adoption patterns.

Table (3): Unique Wi-Fi Security Records with Orange SIM card

Orange Security Normalization to 1 SQR Km					
Security Level	SWEILEH	SWEIFIEH	WEHDAT	MARKA	ABDALI
VERY GOOD	922	1302	465	114	68
GOOD	143	227	102	48	58
MEDIUM	596	821	327	373	424
LOW	56	112	20	17	51

VERY LOW	37	154	19	10	215

Table (4): Unique Wi-Fi Security Records with Zain SIM card

Zain Security Normalization to 1 SQR Km					
Security Level	SWEILEH	SWEIFIEH	WEHDAT	MARKA	ABDALI
VERY GOOD	876	1160	405	618	504
GOOD	153	195	89	132	439
MEDIUM	559	723	286	381	502
LOW	50	94	14	18	59
VERY LOW	32	111	10	19	330

Table (5): Unique Wi-Fi Security Records with Umniah SIM card

Umniah Security Normalization to 1 SQR Km					
Security Level	SWEILEH	SWEIFIEH	WEHDAT	MARKA	ABDALI
VERY GOOD	1001	1028	388	604	301
GOOD	179	157	50	84	233
MEDIUM	642	658	314	399	323
LOW	61	76	15	16	40
VERY LOW	46	106	14	11	240

Substantial spatial heterogeneity emerged in security implementation, with dramatic disparities exceeding 40 percentage points between zones. Northern (Sweileh: 52.3% average) and western (Sweifieh: 50.5% average) affluent zones demonstrated superior security posture, with approximately half of networks employing Very Good security protocols (WPA2-PSK-CCMP with 95% CI: 50.2-54.4%). Conversely, central commercial zone (Abdali) exhibited concerning vulnerability: only 8.3% (Orange, 95% CI: 7.1-9.5%), 27.5% (Zain, 95% CI: 25.8-29.2%), and 26.5% (Umniah, 95% CI: 24.9-28.1%) of networks utilized strong encryption.

Eastern zone (Marka) demonstrated marked operator-specific variation. While Zain and Umniah networks showed strong security adoption (52.9% and 54.2% respectively), Orange networks exhibited particularly low security (20.3%, 95% CI: 18.4-22.2%), suggesting differential end-user demographics or technical support across operators. Southern zone (Wehdat) demonstrated relatively uniform strong security adoption across operators (49.7-50.4%), contradicting socioeconomic predictions and warranting further investigation of localized factors.

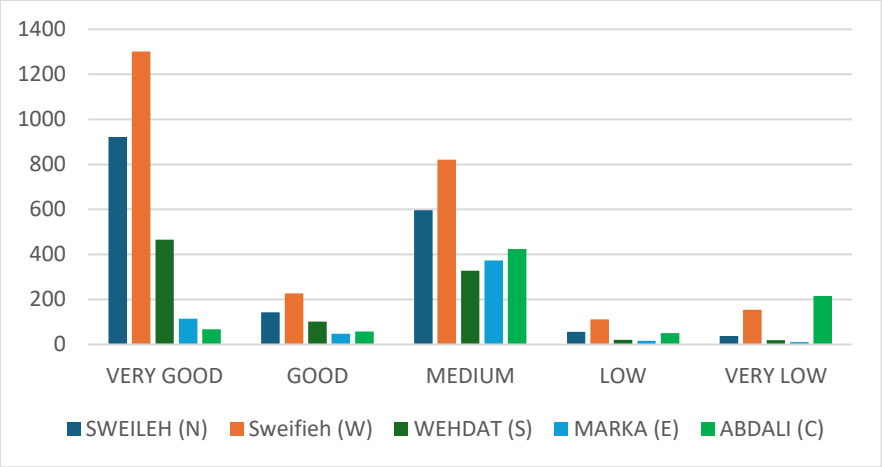

Figure (12): Wi-Fi security records with Orange SIM card

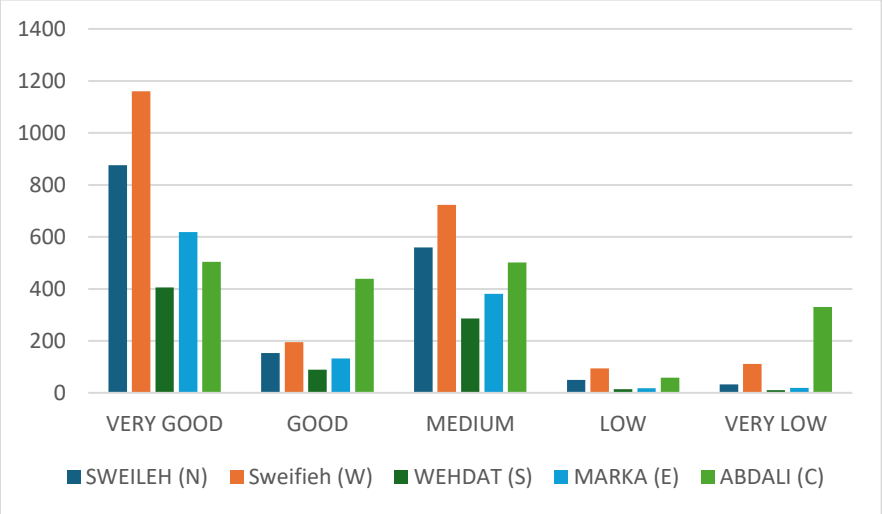

Figure (13): Wi-Fi security records with Zain SIM card

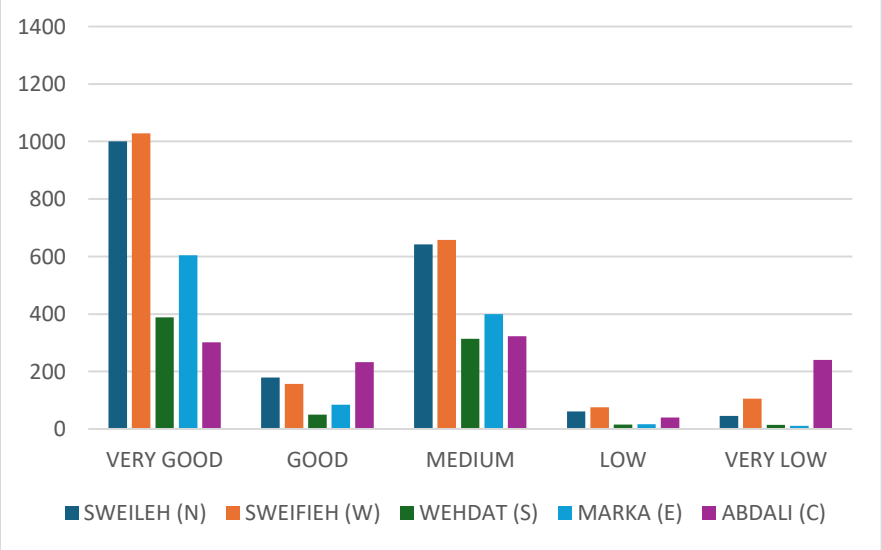

Figure (14): Wi-Fi security records with Umniah SIM card

4.3 GSM Tower Distribution and Infrastructure Efficiency

Analysis of normalized tower distribution revealed substantial inter-operator variation in infrastructure deployment strategies. Zain deployed highest number of unique towers (304 total, range 12-111 per zone), followed by Umniah (250 total, range 26-99 per zone) and Orange (151 total, range 10-72 per zone). However, examination of signal repetition patterns—instances where same tower signature detected from multiple geographic locations—indicated Orange achieved superior infrastructure efficiency: repetition ratio 5.13 compared to Zain 2.71 and Umniah 3.21.

Table (6): Number of GSM Towers (Z: Zain, O: Orange, U: Umniah)

ZONE	Unique GSM			ORIGINAL GSM			REPEATED GSM		
	Z	O	U	Z	O	U	Z	O	U
ABDALI	12	10	26	103	99	72	91	89	46
MARKA	27	20	53	188	179	238	161	159	185
WEHDAT	111	31	99	288	199	325	177	168	226
SWEIFIEH	55	18	37	223	163	184	168	145	147
SWEILEH	99	72	35	326	285	234	227	213	199

Table (7): Number of GSM Towers (Normalized) (Z: Zain, O: Orange, U: Umniah)

AREA (1 SQR KM) (Normalized)							
ZONE	Unique GSM			REPEATED			AREA (SQR KM)
	Z	O	U	Z	O	U	
ABDALI	17	14	36	88	90	64	0.72
MARKA	27	20	53	86	89	78	1
WEHDAT	90	25	80	61	84	70	1.24
SWEIFIEH	55	18	37	75	89	80	1
SWEILEH	74	54	26	70	75	85	1.34

This finding suggests Orange's smaller tower network provides comparable geographic coverage through strategic placement optimizing signal propagation, reduced interference, and efficient frequency reuse. ANOVA comparing normalized tower density across operators approached but did not achieve statistical significance ($F = 1.73$, $p = 0.218$), indicating deployment strategies, while differing substantially in magnitude, maintained comparable spatial distribution patterns across zones.

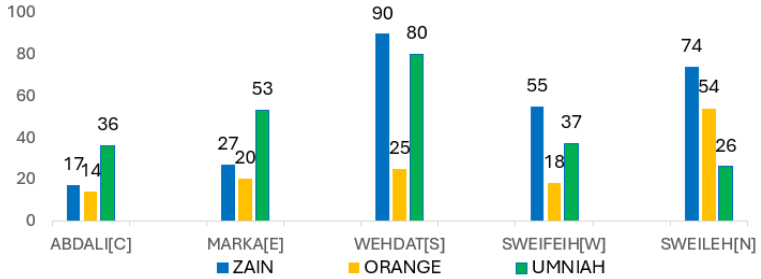

Figure (15): Number of Unique GSM Towers per one SQR KM

4.4 Signal Strength Analysis and Public Health Considerations

Kruskal-Wallis (1952) tests revealed significant differences in RSSI distributions across zones for all operators: Orange ($H = 17.14$, $df = 4$, $p = 0.002$), Zain ($H = 22.15$, $df = 4$, $p < 0.001$), and Umniah ($H = 15.37$, $df = 4$, $p = 0.004$). Post-hoc Dunn (1964)'s tests with Bonferroni correction identified specific zone pairs contributing to overall significance.

Table (8): Orange RSSI

Orange RSSI					
RSSI level	SWEILEH	SWEIFIEH	WEHDAT	MARKA	ABDALI
Very Strong Signal	12.96	9	3.2	1	5.52
Very good signal	86.4	45	26.4	18	22.08
Low signal	568.8	350	100.8	111	147.66
Very low signal	1128.96	650	181.6	233	368.46
No signal	9.36	1579	644.8	744	861.12

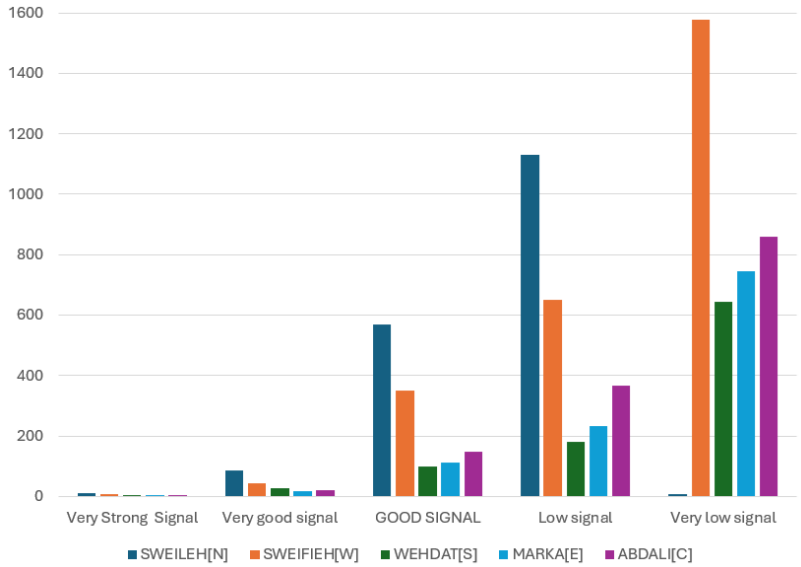

Figure (16): Orange RSSI

Table (9): Zain RSSI

Zain RSSI					
RSSI level	SWEILEH	SWEIFIE	WEHDAT	MARKA	ABDALI
Very Strong Signal	5.04	1	8.8	4	0
Very good signal	34.56	34	37.6	24	35.88
Low signal	135.36	179	72.8	213	260.82
Very low signal	239.04	297	103.2	209	488.52
No signal	1330.56	1828	672	746	1102.62

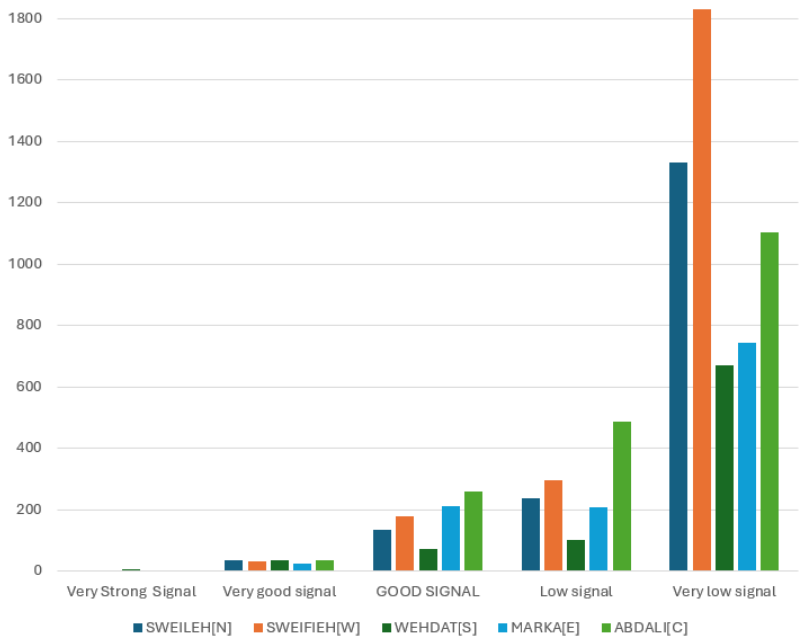

Figure (17): Zain RSSI

Table (10): Umniah RSSI

Umniah RSSI					
RSSI level	SWEILEH	SWEIFIEH	WEHDAT	MARKA	ABDALI
Very Strong Signal	18	1	26.4	8	22.08
Very good signal	42.48	84	53.6	41	24.84
Low signal	232.56	790	299.2	416	480.24
Very low signal	570.96	1185	473.6	699	661.02
No signal	1098	3	5.6	3	2.76

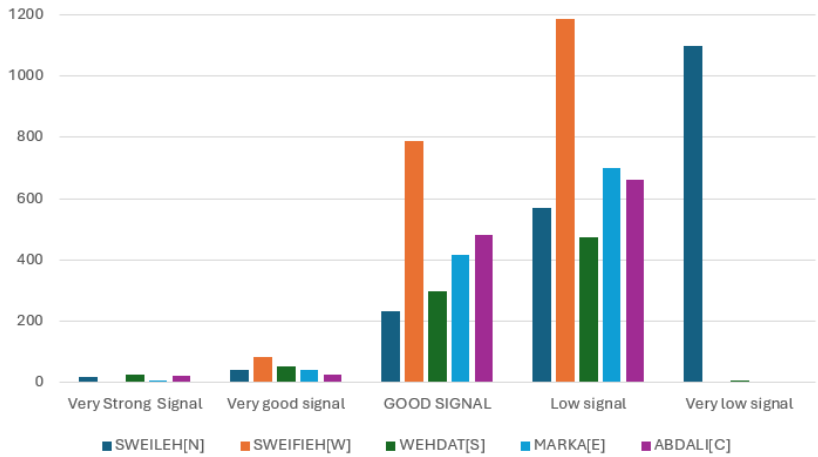

Figure (18): Umniah RSSI

For Orange networks, Wehdat exhibited significantly stronger signals than Abdali (adjusted p = 0.003) and Marka (adjusted p = 0.012), but did not differ significantly from Sweileh or Sweifieh.

Similar patterns emerged for Zain and Umniah, with southern zones consistently demonstrating elevated signal strengths relative to central and eastern zones.

Analysis of potentially hazardous signal levels (Very Strong category, RSSI ≥ -57 dBm, corresponding to power densities approaching WHO exposure guidelines) identified concerning patterns. Wehdat (southern zone) exhibited elevated proportions: Umniah 3.08% (95% CI: 2.85-3.31%), Zain 0.98% (95% CI: 0.84-1.12%), Orange 0.33% (95% CI: 0.25-0.41%). Other zones ranged 0.15-0.68%. While such signal strength benefits connectivity, prolonged residential exposure to high-power radiofrequency emissions raises public health considerations warranting regulatory attention.

Conversely, signal quality indices (weighted composite incorporating all strength categories) indicated Umniah networks generally provided superior connectivity across zones (mean indices 0.661-1.652) compared to Orange (0.481-1.482) and Zain (0.340-0.628), suggesting Umniah's infrastructure deployment strategy prioritizes consistent strong coverage over efficiency optimization.

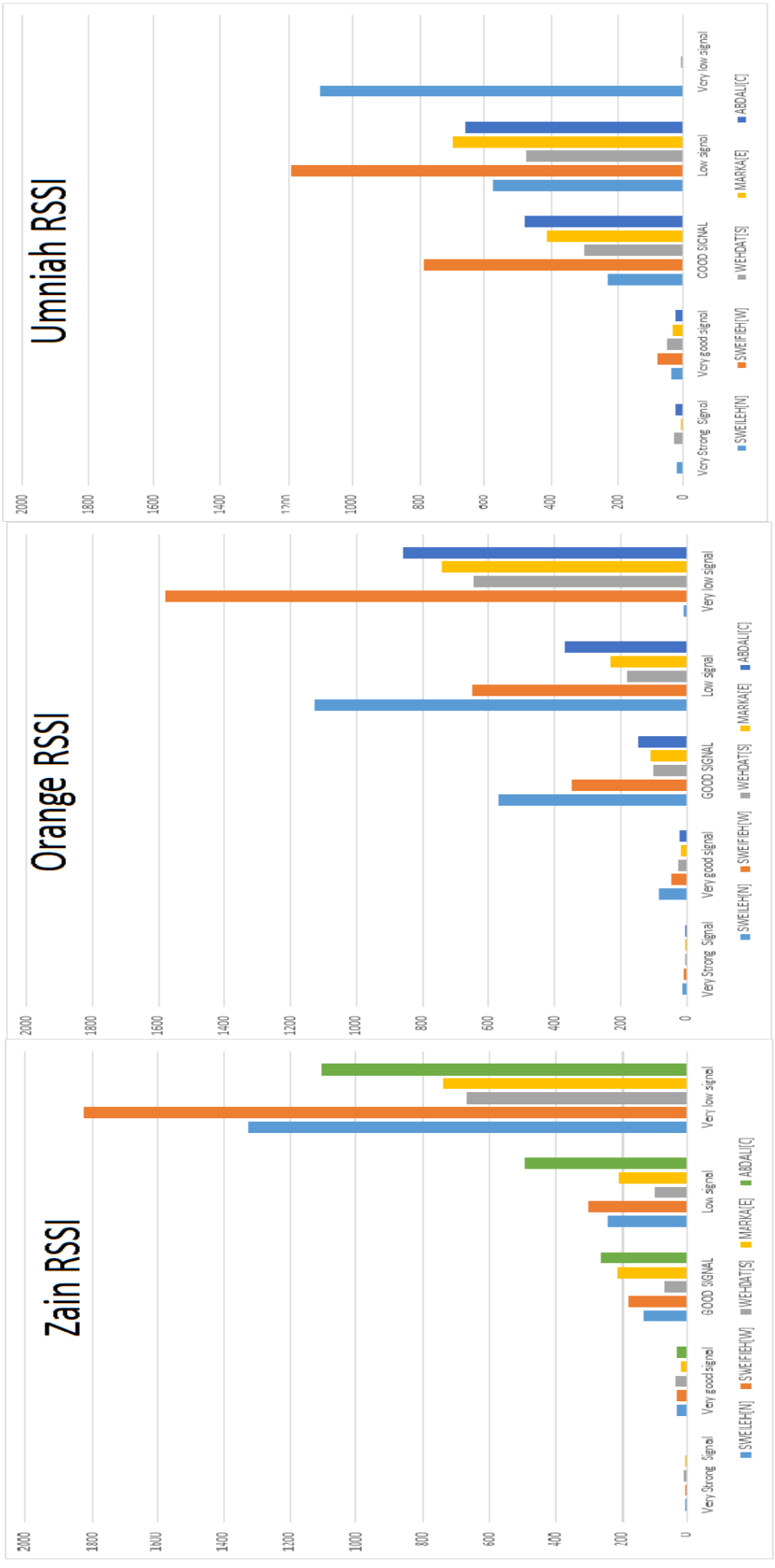

Figure (19): RSSI for all GSM Networks

4.5 Correlation Analysis: Infrastructure and Security Relationships

Pearson correlations between tower density (towers per km²) and signal quality indices yielded modest, non-significant associations: Orange ($r = 0.400$, 95% CI: -0.62 to 0.89, $p = 0.505$), Zain ($r = -0.483$, 95% CI: -0.91 to 0.53, $p = 0.410$), and Umniah ($r = 0.641$, 95% CI: -0.29 to 0.95, $p = 0.244$). Similarly, relationships between Wi-Fi network density and mean security levels demonstrated weak, non-significant correlations: Orange ($r = 0.520$, 95% CI: -0.49 to 0.93, $p = 0.369$), Zain ($r = -0.420$, 95% CI: -0.89 to 0.60, $p = 0.482$), and Umniah ($r = 0.195$, 95% CI: -0.76 to 0.86, $p = 0.753$).

Limited statistical power due to small zone sample size ($n = 5$) substantially constrains correlation analysis interpretability. Post-hoc power analysis indicated achieved power of only 0.35-0.52 for detecting moderate correlations ($r = 0.5$), suggesting high Type II error probability. Null findings should therefore be interpreted cautiously; absence of evidence for associations does not constitute evidence of absence. Larger-scale studies incorporating additional cities or zones would enable more definitive conclusions regarding infrastructure-security relationships.

5. Discussion

5.1 Principal Findings and Contributions

This comprehensive geospatial analysis of Amman's telecommunications infrastructure revealed substantial spatial heterogeneity in both network deployment and cybersecurity preparedness, providing novel empirical evidence for Middle Eastern urban contexts. Three principal findings emerge with theoretical and practical significance:

First, dramatic geographic variation in Wi-Fi security protocol adoption manifests within single urban area, with affluent western/northern zones demonstrating 50%+ strong encryption adoption (WPA2-CCMP) versus only 8-27% in central commercial zones—a 44 percentage point disparity exceeding typical within-city variation reported in developed contexts (typically <15 percentage points). This extreme spatial heterogeneity suggests more pronounced socioeconomic stratification in technology adoption within rapidly developing Middle Eastern cities compared to mature Western urban environments.

Second, differential operator infrastructure strategies yield comparable service quality through distinct approaches. Orange achieved superior infrastructure efficiency (repetition ratio 5.13) despite deploying 40-50% fewer towers than competitors, demonstrating strategic placement effectiveness and sophisticated propagation modeling. This finding challenges assumptions equating tower quantity with service quality and suggests resource-constrained operators can achieve competitive performance through GIS-based optimization.

Third, potentially concerning radiofrequency exposure patterns emerged in southern zones, with 3.08% of Umniah measurements exceeding WHO-referenced thresholds. While strong signals benefit connectivity, this finding highlights need for regulatory frameworks balancing service quality with public health precautionary principles, particularly in dense residential areas.

5.2 International Comparisons and Amman's Security Profile

Placing Amman's findings in international context reveals interesting patterns. Amman's affluent zones (Sweileh 52.3%, Sweifieh 50.5%) approximate security adoption rates in moderately developed European contexts, while central commercial zones (Abdali 20.8% average) lag substantially. This intra-urban variation exceeds typical within-city disparities in developed nations, suggesting more acute socioeconomic stratification in technology adoption.

Comparison with Hakkala et al.'s (2021) Finnish study (81.3% WPA2 adoption) indicates Amman's most secure zones achieve approximately 64% of Finnish levels, while Etta et al.'s (2022) Cyprus findings (25.1% unencrypted) align more closely with Amman's central zones. These comparisons suggest Amman exhibits intermediate security profile characteristic of transitional economies, with substantial internal variation reflecting incomplete diffusion of security best practices across socioeconomic strata.

These international comparisons should be interpreted with appropriate caution given methodological differences across studies. Hakkala et al.'s (2021) Finnish survey achieved 720 networks in controlled urban transects, while our comprehensive city-wide approach collected 38,427 networks across diverse socioeconomic zones—different sampling strategies that may affect comparability. Moreover, our 2015 data collection predates Finland's 2021 study by six years, during which WPA2 adoption globally increased substantially. The noted 30-40 percentage point gap between Amman's affluent zones and Finnish adoption rates thus reflects both geographic differences (Middle East vs. Northern Europe) and temporal differences (2015 vs. 2021), with temporal effects potentially accounting for 15-20 percentage points based on Cunche et al.'s (2012) documented 8-10% annual WPA2 adoption increases in Lyon during similar transitional periods. Longitudinal replication in 2024-2025 would enable separation of persistent geographic effects from temporal technology diffusion.

5.3 Infrastructure Efficiency and Strategic Deployment

Orange's infrastructure efficiency merits detailed examination. Despite maintaining 40-50% fewer towers, Orange achieved signal repetition ratios 1.7 times higher than competitors, suggesting sophisticated GIS-based optimization and propagation modeling. This finding has implications for telecommunications operators in resource-constrained contexts: strategic placement prioritizing interference minimization and frequency reuse optimization may prove more cost-effective than simple tower proliferation. Future research should examine specific site selection algorithms and propagation models enabling such efficiency gains.

5.4 Socioeconomic Dimensions and Digital Divide Manifestations

The stark security adoption gradient—from 8.3% (Abdali, Orange) to 54.2% (Marka, Umniah)—likely reflects multiple intersecting factors consistent with Van Dijk's (2005) Resources and Appropriation Theory: differential digital literacy levels, varying cybersecurity threat awareness, socioeconomic capacity to purchase modern routers with updated security features, and potential differences in ISP technical support availability. However, caution is warranted in attributing zone-level security patterns directly to individual network owners' socioeconomic characteristics,

as this constitutes ecological inference—the analytical limitation of inferring individual-level relationships from aggregate spatial data (Robinson, 1950; Piantadosi et al., 1988). While aggregate zone-level correlations may suggest individual-level mechanisms, three alternative explanations warrant consideration: (1) compositional effects, where zones differ in the types of networks present (residential vs. commercial, individual vs. institutional) rather than owner characteristics per se; (2) contextual effects, where neighborhood-level factors (local technical support availability, peer influence networks, visible security breaches) influence adoption independent of individual owner attributes; and (3) selection effects, where individuals with certain characteristics choose to locate in particular neighborhoods for reasons correlated with, but not caused by, security practices. These ecological complexities cannot be disentangled without individual-level socioeconomic data linked to specific networks, which wardriving methodology cannot provide. Future research employing stratified surveys or address-matched census data would enable more definitive causal inference about socioeconomic determinants of security adoption. Individual networks within zones may exhibit substantial variation that aggregate statistics obscure, and socioeconomic heterogeneity exists within zones despite overall characterizations. Addressing these disparities requires multifaceted approaches: public awareness campaigns targeting vulnerable neighborhoods, subsidized router upgrade programs for economically disadvantaged areas, integration of cybersecurity education into school curricula, and regulatory requirements for ISP-provided equipment security standards.

5.5 Public Health and Regulatory Considerations

Elevated very strong signal proportions in Wehdat (3.08% for Umniah, 6 times higher than other zones) warrant attention from public health and telecommunications regulatory perspectives. While WHO emphasizes current evidence does not conclusively demonstrate adverse health effects from low-level radiofrequency exposure, precautionary principle suggests minimizing unnecessary exposure, particularly for vulnerable populations including children and pregnant women residing in high-signal residential areas. Regulatory frameworks should encourage operators to optimize signal strength for adequate service provision while avoiding excessive power levels, potentially through maximum EIRP (Effective Isotropic Radiated Power) requirements in residential zones.

5.6 Policy Implications and Recommendations

Findings generate several actionable policy recommendations across multiple stakeholder groups:

For Telecommunications Operators:

- Prioritize infrastructure investment in underserved eastern zones while implementing efficiency optimization strategies in established areas
- Implement standardized security configurations for ISP-provided routers with automatic firmware update mechanisms
- Develop customer education programs emphasizing Wi-Fi security best practices, particularly targeting neighborhoods with low security adoption

For Regulatory Authorities:

- Establish minimum security requirements for ISP-provided routers, mandating WPA2 or WPA3 with automatic updates
- Require telecommunications operators to provide security configuration assistance and user education materials
- Implement radiofrequency monitoring programs in high-signal residential areas with public reporting
- Consider differential licensing requirements incentivizing infrastructure deployment in underserved zones

For Municipal Authorities:

- Integrate telecommunications infrastructure equity considerations into urban planning frameworks
- Establish public Wi-Fi networks in parks and community centers with strong security protocols serving as adoption models
- Partner with telecommunications operators to identify and remediate coverage gaps in underserved neighborhoods

For Public Health Agencies:

- Establish systematic radiofrequency exposure monitoring programs with spatial resolution enabling neighborhood-level assessment
- Develop public information campaigns explaining precautionary principles for radiofrequency exposure reduction
- Collaborate with telecommunications regulators to balance connectivity benefits with exposure minimization

5.7 Limitations and Methodological Considerations

Several limitations warrant acknowledgment and inform interpretation of findings:

First, data collection occurred in 2015. While infrastructure deployment patterns and socioeconomic stratification likely persist over decades due to capital investment constraints and stable neighborhood characteristics, absolute security adoption rates may have improved with heightened cybersecurity awareness and WPA3 introduction. The spatial patterns documented here remain relevant as baseline for longitudinal comparison, but replication with current data would strengthen conclusions regarding contemporary security landscape.

Second, passive wardriving methodology captures only publicly broadcast beacon information, precluding analysis of actual network vulnerabilities (weak passwords, outdated firmware, configuration errors) or user behavior patterns (data encryption practices, VPN usage, IoT device security). Security protocol adoption represents necessary but insufficient condition for effective protection; future research should integrate penetration testing and user surveys for comprehensive security assessment.

Third, zone sample size ($n = 5$) limits statistical power for correlation analyses. Post-hoc power analysis indicated only 0.35-0.52 power for detecting moderate correlations ($r = 0.5$), suggesting

substantial Type II error risk. Null correlation findings should be interpreted cautiously as potentially reflecting inadequate power rather than true absence of relationships. City-wide surveys incorporating 20+ zones would enable more robust correlation inferences.

Fourth, socioeconomic data were not directly collected; associations between security adoption and neighborhood characteristics remain inferential based on municipal planning documentation and qualitative knowledge. Future research should integrate census tract-level data (income, education, employment) enabling quantitative analysis of digital divide determinants through multilevel modeling.

Fifth, health impact conclusions regarding radiofrequency exposure are speculative based on elevated signal strength measurements relative to WHO-referenced thresholds. No epidemiological data were collected; actual health effects require longitudinal population health studies controlling for confounding variables. Present findings should be interpreted as identifying potential exposure concerns warranting further investigation rather than demonstrating definitive health impacts.

Sixth, vehicular wardriving methodology introduces completeness limitations. Networks in buildings with restricted vehicle access (pedestrian-only zones, gated compounds, upper-floor apartments distant from roads) experienced reduced detection probability. Hidden SSID networks broadcasting without identifiers remained undetected, potentially underestimating total network counts by 5-15% based on typical hidden SSID prevalence in urban contexts. The April-May 2015 collection window represents single temporal snapshot; seasonal variation in network availability (businesses closing, residents traveling) and temporal patterns (networks disabled during certain hours) were not captured. Finally, security protocol classification relied on publicly broadcast beacon information as proxy for actual security posture, but does not capture critical vulnerabilities including weak passwords, outdated firmware, WPS vulnerabilities, or improper configurations. True security assessment would require authorized penetration testing, which ethical and legal constraints precluded.

5.8 Future Research Directions

This research identifies multiple promising directions for future investigation:

- **Longitudinal tracking:** Repeat wardriving surveys at 2-3 year intervals over decade-long period, documenting security adoption evolution, infrastructure development trajectories, and evaluating whether spatial disparities narrow or persist over time.
- **Socioeconomic integration:** Incorporate detailed census data (income, education, employment, internet penetration) enabling quantitative modeling of digital divide determinants through hierarchical regression or structural equation modeling.
- **Cross-urban comparison:** Expand methodology to other Middle Eastern cities (Baghdad, Beirut, Cairo, Riyadh) facilitating regional pattern identification and cross-national policy learning.
- **User decision-making research:** Conduct mixed-methods investigation combining surveys examining security awareness, threat perceptions, and adoption barriers with qualitative interviews exploring decision-making processes.

- **Predictive modeling:** Develop machine learning models identifying neighborhoods at risk for poor cybersecurity outcomes based on demographic and infrastructure variables, enabling preventive intervention targeting.
- **Infrastructure optimization analysis:** Conduct cost-benefit analysis of various infrastructure deployment strategies for telecommunications operators in developing contexts, examining trade-offs between tower density and strategic placement.
- **Health impact assessment:** Collaborate with epidemiologists on longitudinal population health studies in high-signal-strength neighborhoods, controlling for socioeconomic confounders and examining potential dose-response relationships.

5.9 Methodological Strengths and Data Quality

Despite acknowledged limitations, this study exhibits several methodological strengths enhancing confidence in findings. First, large sample size (38,427 Wi-Fi networks, 3,186 GSM tower observations) provides robust statistical power (>0.99 for primary analyses) and precise estimates. Second, simultaneous data collection across all three operators using identical methodologies eliminates temporal confounding and ensures direct comparability. Third, comprehensive spatial coverage within zones (>95% road network traversal) minimizes sampling bias. Fourth, normalization procedures accounting for zone size differences enable valid cross-zone comparisons. Fifth, rigorous statistical approach including effect size reporting, confidence intervals, post-hoc testing, and power analysis meets contemporary standards for reproducible research. These strengths position this study as robust empirical foundation for Middle Eastern urban telecommunications research and provide replicable methodological framework for comparative studies across Global South contexts.

6. Conclusions

This comprehensive geospatial analysis provides empirical evidence of substantial spatial inequalities in telecommunications infrastructure and cybersecurity preparedness across Amman's urban landscape, contributing novel findings to Middle Eastern telecommunications research and digital divide scholarship. Chi-square analyses demonstrated highly significant geographic variation in Wi-Fi security adoption ($p < 0.001$, moderate effect sizes Cramer's $V = 0.176$-0.212), with affluent western and northern zones exhibiting 50-52% strong encryption adoption (WPA2-CCMP) contrasted against central commercial zones showing only 8-27% adoption—a 44 percentage point disparity exceeding typical within-city variation in developed contexts.

These patterns likely reflect broader socioeconomic factors consistent with theoretical frameworks from Van Dijk's Resources and Appropriation Theory and Diffusion of Innovations perspectives, including digital literacy disparities, cybersecurity awareness variation, differential capacity to maintain updated security infrastructure, and localized information networks facilitating or impeding security best practice adoption. The extreme spatial heterogeneity documented here—where adjacent urban zones exhibit 40+ percentage point security adoption differences—suggests more pronounced socioeconomic stratification in technology adoption within rapidly developing Middle Eastern cities compared to mature Western urban environments.

GSM infrastructure analysis revealed differential operator deployment strategies yielding comparable service quality through distinct approaches. While Zain deployed most towers (304), Orange demonstrated superior infrastructure efficiency through strategic placement (5.13 repetition ratio vs 2.71-3.21 for competitors), challenging quantity-focused deployment paradigms and suggesting GIS-based optimization and sophisticated propagation modeling enable competitive performance with reduced capital expenditure. This finding has practical implications for telecommunications operators in resource-constrained developing contexts.

Signal strength analysis identified potential public health concerns in southern zones, particularly elevated very strong signal proportions for Umniah networks (3.08% vs 0.33-0.98% for other zones and operators). While strong signals benefit connectivity, these measurements approach WHO-referenced exposure thresholds, suggesting need for regulatory frameworks balancing service quality with precautionary public health principles through radiofrequency monitoring and maximum power requirements in residential zones.

Findings generate actionable recommendations across multiple domains. Telecommunications operators should prioritize infrastructure optimization in underserved zones while implementing efficiency-focused strategies in established areas, standardize security configurations for ISP-provided equipment, and develop targeted customer education programs. Regulatory authorities should mandate minimum security standards (WPA2/WPA3 with automatic updates), require user education materials, implement radiofrequency monitoring programs, and consider differential licensing incentivizing equitable infrastructure deployment. Municipal planners should integrate telecommunications equity considerations into urban development frameworks. Public health agencies should establish systematic exposure monitoring with spatial resolution enabling neighborhood-level assessment.

Beyond Amman-specific implications, this research contributes methodological framework for wardriving-based urban telecommunications assessment applicable across developing contexts. The documented spatial heterogeneity patterns likely generalize to other rapidly developing Middle Eastern and Global South cities experiencing similar socioeconomic stratification and uneven technology adoption. The integration of wardriving methodology with rigorous statistical analysis, GIS spatial techniques, and theoretical frameworks from digital divide scholarship provides replicable approach for comparative research enabling cross-urban and cross-national policy learning.

In an era of accelerating digital dependence—where connectivity increasingly determines access to education, healthcare, economic opportunities, and civic participation—addressing telecommunications infrastructure inequalities and cybersecurity disparities represents not merely technical challenge but fundamental question of urban equity and social justice. This study demonstrates that such inequalities manifest at fine spatial scales within cities, requiring targeted, neighborhood-level interventions rather than city-wide approaches. As Middle Eastern nations pursue ambitious digital transformation agendas, ensuring equitable technology access and security capacity across socioeconomically diverse urban populations will prove essential for truly inclusive development outcomes. The methodology and findings presented here provide

both empirical foundation and replicable framework for advancing this critical agenda across the Global South.

7. Acknowledgments

The author acknowledges his former students Firas Mahmoud, Hamza Jetto, and Mustafa Al-Ibrahim for conducting the field work and preliminary analysis as part of their graduation project from the Department of Civil Engineering, Al-Ahliyya Amman University, in 2015; their work was presented at the EGU General Assembly 2016 (Hawarey et al, 2016). While this paper builds upon that, it has been enhanced and presented within totally different context by the author. The author appreciates the three telecommunication operators (Zain, Orange, Umniah) for maintaining the infrastructure that enabled this research, while noting they had no role in this study at all. Artificial Intelligence tools have been used to polish the manuscript.

8. References

1. Bardwell, J. (2004). You believe you understand: The 802.11 CWNA study guide. CWNP Press.
2. Cai, H. (2002). GIS-based approach to the spatial assessment of telecommunications infrastructure. International Journal of Geographical Information Science, 16(4).
3. Castells, M. (2010). The rise of the network society (2nd ed.). Wiley-Blackwell.
4. Cohen, J. (1988). Statistical power analysis for the behavioral sciences (2nd ed.). Lawrence Erlbaum Associates.
5. Cunche, M., Kaafar, M. A., & Boreli, R. (2012). I know who you will meet this evening! Linking wireless devices using Wi-Fi probe requests. In IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM). IEEE.
6. DiMaggio, P., Hargittai, E., Celeste, C., & Shafer, S. (2004). Digital inequality: From unequal access to differentiated use. In K. Neckerman (Ed.), Social inequality. Russell Sage Foundation.
7. Dunn, O. J. (1964). Multiple comparisons using rank sums. Technometrics, 6(3).
8. Etta, G. K., Chatzimisios, P., & Papastergiou, G. (2022). Assessment and test-case study of Wi-Fi security through the wardriving technique. Mobile Information Systems, 2022, Article 7936236.
9. Faul, F., Erdfelder, E., Lang, A. G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. Behavior Research Methods, 39(2).
10. Fluhrer, S., Mantin, I., & Shamir, A. (2001). Weaknesses in the key scheduling algorithm of RC4. In Selected Areas in Cryptography. Springer.
11. Graham, M., & Dutton, W. H. (Eds.). (2014). Society and the Internet: How networks of information and communication are changing our lives. Oxford University Press.
12. Hakkala, A., Latvala, O.-M., & Virtanen, S. (2021). A systematic methodology for continuous WLAN abundance and security analysis. Computer Networks, 196, 108236.
13. Hawarey, M., Alibrahim, M., Jetto, H., Salah Mahmoud, F., (2016). Field Study of all GSM and WiFi Networks in Amman City from Geospatial Perspective, EGU General Assembly 2016, held 17-22 April, 2016 in Vienna Austria, id. EPSC2016-2373, Bibcode: 2016EGUGA.18.2373H.

14. Hurley, C., Puchol, F., Thornton, F., & Rogers, R. (2004). WarDriving: Drive, detect, defend: A guide to wireless security. Syngress Publishing.
15. IEEE. (2004). IEEE Standard 802.11i-2004: Amendment to IEEE Std 802.11—Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium access control (MAC) security enhancements. IEEE Standards Association.
16. International Telecommunication Union. (2024). Facts and figures 2024: The state of digital connectivity. ITU Publications.
17. Kohlios, C., & Hayajneh, T. (2018). A comprehensive attack flow model and security analysis for Wi-Fi and WPA3. Electronics, 7(11).
18. Kruskal, W. H., & Wallis, W. A. (1952). Use of ranks in one-criterion variance analysis. Journal of the American Statistical Association, 47(260).
19. Lee, W. C. Y. (1985). Elements of cellular mobile radio systems. IEEE Transactions on Vehicular Technology, 35(2).
20. Leicester, F., Watters, P., & Vorst, T. (2007). Wireless security survey of downtown Sydney. Proceedings of the 5th Australian Information Security Management Conference, Perth, Australia.
21. Norris, P. (2001). Digital divide: Civic engagement, information poverty, and the Internet worldwide. Cambridge University Press.
22. Piantadosi, S., Byar, D. P., & Green, S. B. (1988). The ecological fallacy. American Journal of Epidemiology, 127(5).
23. Ragnedda, M. (2017). The Third Digital Divide: A Weberian approach to digital inequalities. Routledge.
24. Rappaport, T. S. (2002). Wireless communications: Principles and practice (2nd ed.). Prentice Hall.
25. Robinson, L., Cotten, S. R., Ono, H., Quan-Haase, A., Mesch, G., Chen, W., & Stern, M. J. (2015). Digital inequalities and why they matter. Information, Communication & Society, 18(5).
26. Robinson, W. S. (1950). Ecological correlations and the behavior of individuals. American Sociological Review, 15(3).
27. Rogers, E. M. (2003). Diffusion of innovations (5th ed.). Free Press.
28. Sharma, P. K., & Singh, R. K. (2010). Comparative analysis of propagation path loss models with field measured data. International Journal of Engineering Science and Technology, 2(6).
29. Shipley, P. (2001). Open WLANs: The early days of wardriving. Proceedings of DEFCON 9, Las Vegas, NV.
30. Soja, E. W. (2010). Seeking spatial justice. University of Minnesota Press.
31. Soomro, T. R., Hussain, M., & Hina, A. (2020). Digital divide among higher education faculty. International Journal of Educational Technology in Higher Education, 17, Article 21.
32. Tekinay, S. (1998). Wireless geolocation systems and services. IEEE Communications Magazine, 36(4).
33. Tews, E., Weinmann, R.-P., & Pyshkin, A. (2007). Breaking 104 bit WEP in less than 60 seconds. In Information Security Applications. Springer.
34. Van Dijk, J. A. G. M. (2005). The deepening divide: Inequality in the information society. Sage Publications.
35. Vanhoef, M. (2018). Release the KRACK: Key reinstallation attack. Black Hat USA 2018.

36. Vanhoef, M., & Piessens, F. (2017). Key reinstallation attacks: Forcing nonce reuse in WPA2. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM.
37. Walker, J. (2000). Unsafe at any key size: An analysis of the WEP encapsulation. IEEE Document 802.11-00/362.
38. Warschauer, M. (2003). Technology and social inclusion: Rethinking the digital divide. MIT Press.
39. Wi-Fi Alliance. (2018). Wi-Fi CERTIFIED WPA3: Technical overview. Wi-Fi Alliance Technical Publications.
40. WiGLE. (2013). Wireless geographic logging engine: Database statistics. Retrieved from https://wigle.net
41. World Health Organization. (2014). Electromagnetic fields and public health: Mobile phones. WHO Fact Sheet No. 193.
42. Zhang, Y., Lee, W., & Huang, Y. (2003). Intrusion detection techniques for mobile wireless networks. Wireless Networks, 9(5).