Received March 5, 2019, accepted April 10, 2019, date of publication April 16, 2019, date of current version April 30, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2911675

Exploiting High Millimeter Wave Bands for Military Communications, Applications, and Design

JAMES F. HARVEY[1], (Fellow, IEEE), MICHAEL B. STEER[2], (Fellow, IEEE), AND THEODORE S. RAPPAPORT[3], (Fellow, IEEE)
[1]U.S. Army Research Office, Arlington, VA 22203, USA
[2]Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27695, USA
[3]Tandon School of Engineering, New York University, Brooklyn, NY 11201, USA

Corresponding author: Michael B. Steer (mbs@ncsu.edu)

ABSTRACT Military communications networks can leverage much of the millimeter-wave (mm-wave) technology being investigated and developed for 5G cellular but require special attention to the unique military requirements. This paper highlights the special communications' requirements of specific military local area networks and discusses how higher band mm-wave technology can contribute to high data rates and simultaneously achieve covertness. Adaptive tuning for varying atmospheric absorption meets the military requirements for quickly adjusting covert communication zones to accommodate potentially rapid movements of network nodes, dynamic output power constraints, and changing environmental conditions.

INDEX TERMS 5G, military communications, millimeter-wave propagation.

I. INTRODUCTION

Military communications networks can leverage much of the millimeter-wave (mm-wave) technology being investigated and developed for 5G cellular, but require special attention to the unique military requirements. Military local area networks (LANs) designed for mobile command posts and unmanned aerial vehicle (UAV) swarms, for example, have highly dynamic geometric configurations and require adaptive covertness and jam resistance not demanded by most 5G applications, while still needing to maintain the ultra-high bandwidth and new lower latencies provided by 5G. Many 5G systems exploit the high bandwidths available at the higher mm-wave frequencies, increasing the capacity further by using beam-steering and massive multiple-input and multiple output (MIMO) techniques. This paper highlights the special communications requirements of specific military LANs and discusses how higher band mm-wave technology can contribute to their solution. The paper reviews the contribution to higher signal to noise ratios (and therefore channel capacity) that is available by moving up to millimeter frequencies, and explodes the commonly-held belief that mm-wave links offer less power over distance than conventional microwave or UHF links. In fact, we show fundamentally that this myth is in error, and, ignoring weather effects, that greater, and not poorer, link margins result at mm-wave frequencies when array antennas are used, a point not widely understood until it was demonstrated in recent 5G investigations [1]–[6]. While others have pointed out the covertness advantages of operating near atmospheric absorption lines in the higher mm-wave region, e.g. [7]. this paper emphasizes the special advantages of adaptive tuning along these absorption lines to meet military requirements for quickly adjusting covert communication zones to accommodate potentially rapid movements of network nodes, dynamic output power constraints, and changing environmental conditions.

Communications link path loss is a major consideration in designing communications networks. A common misconception is that higher mm-wave frequencies are not appropriate for outdoor LAN applications due to excessive path loss and weather effects [8]. We note that when a communications link uses antennas that consist of single-element resonant antennas (such as resonant dipoles) the free space path loss increases with frequency because the physical size and therefore the effective aperture area (A_e) of the antennas decrease

The associate editor coordinating the review of this manuscript and approving it for publication was Vittorio Degli-Esposti.

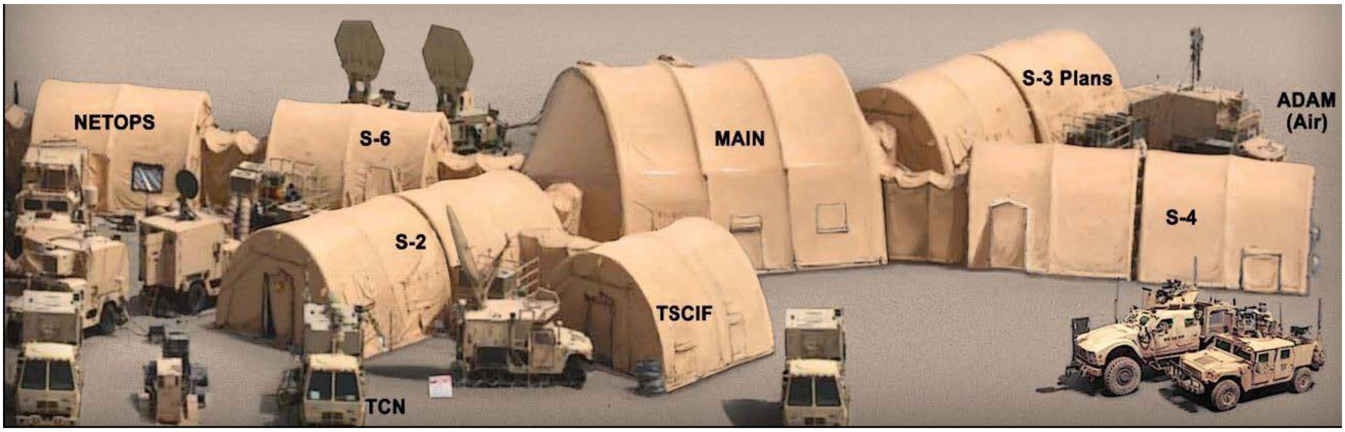


FIGURE 1. Example of brigade command post [10]. U.S. Federal Government work not subject to copyright.

with frequency. This situation, one of a shrinking antenna to maintain constant gain as frequencies increase, makes the use of higher mm-wave frequencies practical only for very short links and small networks. However, for most real world applications, the physical space available for the antenna is fixed by the size of the network node platform, and antenna arrays can exploit the available physical area to accommodate a larger number of array elements at higher frequencies. Therefore, higher gain antennas and more highly directive links occur at higher frequencies. In this case the reverse conclusion is drawn: the propagation conditions improve significantly for higher mm-wave frequencies on a per-area comparison, when weather effects are ignored [1]–[3], [5], [6], since the gain of an antenna with a fixed physical size scales with the square of the frequency, as discussed in [1], [2] and in more detail below. The high bandwidth and data rates possible at the higher mm-wave frequencies, due to the narrower beamwidths obtained with high gain antenna arrays, offer the opportunity for a dynamically adaptive covert, jam-resistant network, and the more favorable link budgets which are essential to a number of military system applications.

II. MILITARY MILLIMETER WAVE COMMUNICATION NEEDS

Many of the military needs for mm-wave communications parallels that of the commercial world but with the added requirements of covertness and resistance to intentional jamming signals, and a higher priority paid to being tamper-proof. This section describes the changing military environment and new communication needs that are driving hardened military millimeter-wave communications.

A. WIRELESS LAN FOR TACTICAL COMMAND POST AND FIELD HEADQUARTERS

Military doctrine is changing to emphasize extreme flexibility and rapid operations. The Russian military was the first to articulate what they called the ‘‘reconnaissance-strike complex,’’ which combined technology developments in sensors and command and control networks with precision guided munitions to achieve strategic breakthroughs in the real-time precision targeting of ground forces [9]. However, the US military was the first to weaponize and field this concept in the latter years of the cold war. Russia has recently modernized its military forces and has implemented this concept of warfighting, in particular an ‘‘anti-access, area denial’’ (A2/AD) capability. China is also actively incorporating the concept as part of its A2/AD capability. The result of these developments by China, Russia, and the US, as well as by their allies, means that future large-scale conflicts will be extremely violent and/or fast paced. To be successful, one adversary will need to get inside the decision loop of its opponents. This will require extreme agility, rapid movement, and swift reaction times on the battlefield. It becomes necessary to significantly reduce the time to deploy and relocate forces.

The most vulnerable assets in a battlefield engagement are the battlefield headquarters and command posts. Traditionally these are relatively fixed elements, being slow to set up, not designed to be moved often, and not designed to be mobile. In the future, these elements need to move fast, often, and suddenly, in order to survive. Fig. 1 shows a command post of an army brigade, a self-contained combat unit typically commanded by a colonel and having independent communications, intelligence, logistics and weapons systems coordinating the battle with up to 11,000 (but more usually 3,000 to 5,500) soldiers and comprehensive weapon systems. The brigade command post incorporates substantial computing capabilities and receives enormous amounts of data, particularly visual, image, map, and streaming video. Furthermore, this data must be exchanged among the headquarter's staff. The massive amounts of data expected to be generated by the exploding number of sensors, and the need to make the data available to an increasing number of decision makers, coupled with the introduction of artificial intelligence (AI) to assist humans in making timely decisions, drives the need for increasingly complex fast integrated communications networks. The evolving information cloud will require very high (multi gigabit/s or more) data rate information transfers between servers in the command post [11]. Virtual reality enabled by these developments will give commanders and staff officers a new capability to virtually visit subordinate units [11].

The command post shown in Fig. 1 is a recent example of an element that has been considerably down-sized physically (reducing its footprint), technology up-graded, modularized, and designed for rapid tear-down and re-build. Yet it is still an "... unwieldy nest, strung with hundreds of feet of cable, stacked with towers of transit cases, and populated by a jumble of computers, connectors, servers, and ..." as many as 300 terminals [10], [12], [13]. It is big, with a large visual signature, it looks like a command post, and it takes too much manpower and transportation capacity. The command post shown in Fig. 1 takes a platoon (roughly 30 soldiers) a day to install or dismantle. This is far too slow for the command post of the future that requires agile deployment and even continuously mobile operation. A high capacity, high bandwidth, wireless LAN will eliminate the cables and connections and would allow for quick installation/dismantling, and for headquarters elements to be dispersed, thus decreasing their visual footprint and vulnerability to attack. Furthermore, such a network would support on-the-move headquarters operations necessary to maintain extremely fast tactical operations stressing an adversary's ability to tactically react effectively. This then becomes one element of getting inside an adversaries decision loop. "On the future battlefield, if you stay in one place longer than two or three hours, you will be dead [14]." A high capacity back-haul link would also be needed to communicate with higher and lower headquarters and with tactical elements. This WLAN capability is being explored as part of the Warfighter Information Network-Tactical (WIN-T) program, increments 1 and 2 [15].

Both the LAN and the back-haul link could introduce electromagnetic vulnerability [16]. Clearly using cables renders the command, control and communications system much more tamper-resistant than a WLAN system and replacing cables with a WLAN provides a rich target for cyberattack. Security of the WLAN, especially resistance to wireless hacking, eavesdropping, and intentional electronic jamming, are of paramount concern, and hence the LAN must be covert and resistant to electronic jamming and hacking. The covert coverage must be adaptive in real time to expand links to accommodate the changing positions of the headquarters and changing atmospheric conditions.

These concerns imply that the military exploitation of mm-wave communications has different priorities than do commercial applications.

B. MILITARY LEAPFROG

A military, in developing its reconnaissance and strike network and A2/AD capabilities, strives to render obsolete an adversary's precision weapons and weaponization of information. One way, adopted by the US military, of staying ahead of this threat environment is by the development of extremely high quality and increasingly expensive weapons systems. This rising cost has caused a rethinking of US strategy. It has been pointed out that the cost of military aircraft is increasing exponentially, while defense budgets are only growing linearly (at best) [17]. Current military thinking and planning is looking at optimal mixes of high quality, high cost systems with lower cost, lower quality, but more numerous systems.

It is being recognized that quantity has its own measure of quality. For example, consider two fencers of equal ability. One might expect that each fencer would win roughly 50% of their bouts. But add an additional fencer to one side and the larger side would win nearly 100% of the bouts, provided there is effective communication between the two fencers and an increased information processing capability to respond to a more complex tactical situation, rather than the 66% win rate from a simple linear analysis. This type of analysis has been extended to the outcome of a military engagement and encapsulated in Lanchester's Square Law [18], [19]. Lanchester's Square Law was formulated to analyze relative strengths of military forces, and posits that for forces armed with firearms engaged with another distant force also armed with firearms, the relative strength is proportional to the square of the number of weapons. Lanchester's analysis did not consider coordination between the shooters, which would result in even greater non-linearity. In a 2009 RAND study of a US-Mainland China air engagement over Taiwan, with US fighters estimated to be 27 times better than the opposing more numerous fighters, China launched 800 sorties in the first day and won [9], [20]. Reliance on a large numbers of lower quality weapons systems yields a more graceful degradation than relying on a smaller number of higher quality similar weapons. In order for this approach to be effective there must be high quality wireless communications between the elements and these must be immune from hacking and jamming. Clearly these communications would be a prime target for attack and the level of effort that would be expended to render communications ineffective would be far greater than that which would be used to hack commercial communications. Millimeter-wave communications is a prime candidate for providing the high capacity, covert and jam resistant wireless link needed to mitigate such attacks.

C. NETWORKED ROBOTS AND ROBOTIC SWARMS

An example deployment of the concept discussed in the previous section is the use of relatively less expensive robots, including UAVs, to take on battlefield tasks, the use of man-machine coordination with robots, and deployment of the robot swarming concept (Fig. 2 shows an example of swarming UAVs). This is as an alternative to using fewer more expensive but much more capable robots.

UAV swarms, autonomous or manually operated at stand-off distances, are expected to overwhelm relatively fewer piloted aircraft, air defenses, anti-ship missile systems, and missile emplacements. The use of swarms underpins A2/AD capabilities [22], [23]. News reports describe effective use

FIGURE 2. Example of coordinated UAV swarm [21]. U.S. Federal Government work not subject to copyright.

of drone swarms against Russian air defenses in Syria and against the Patriot missile system in the United Arab Emirates [24]. The US and China are known to be prioritizing their development [23], [25]. Expendable swarming robots can be equipped with lethal or non-lethal munitions, an EM jamming or hacking capability [26], decoy technology, navigation spoofing systems, cyberattack technology [27], or advanced sensors for intelligence, surveillance, and reconnaissance.

Autonomous and semi-autonomous swarms operating far forward with greater persistence and range would enable faster paced operations with better intelligence, coordination, and strategic surveillance supporting ballistic missile defense, e.g. surveillance of North Korean launch facilities [28]. Swarms are also a potential defense against hostile robot swarms of an adversary. It has been shown that ultra-cheap 3D-printed mini-drones costing less than a dollar each deployed in the billions could be fielded successfully against more capable but fewer targets [29].

Demographic changes mean that most of the populace will soon live in mega-cities and therefore future conflicts are likely to be in urban areas [30]. Clouds of drones could sweep buildings or other areas to identify and locate inhabitants as well as weapons systems [9]. With high capacity communications between the elements of the swarm and large computational capabilities on board, the swarm can collectively develop images of large structures and of enemy positions. A greater combat capability would result from an ability for distributed, cooperative computing and information processing among the swarm elements, e.g. to enable real time formation adjustment, collective decision making, advanced image processing and target analysis, and the exploitation of advanced artificial intelligence algorithms [31]. Forward information processing within the swarm, and high capacity intra-swarm communications is important to reduce the back-haul communications requirement to controller facilities [27]. Ground robots and maritime robots can also be employed in swarms to similar advantage and in cross-domain swarms combining ground, aerial, and maritime robots [32]–[34]. All the swarming capability discussed above depends on very high capacity, covert, jam-resistant communications between swarm elements. In particular, insurgents have demonstrated that UAVs are vulnerable to capture by hacking [35].

D. PROPOSED MILITARY WIRELESS APPLICATIONS

Many military applications have been proposed where a high capacity, adaptively covert, and jam-resistant wireless link can add significant capability, but will not require the same high data rate communications as the future command post or swarming robots. These include: small unit LAN communications [7], [36], communications with a stealthy aerial refueler [32], control of unmanned aerial resupply (including blood delivery) vehicles [37], [38], a wireless launcher-missile interface to exchange prelaunch systems health and targeting information along with post-launch guidance [39], control of a robotic wingman [40], support of manned-unmanned teaming [41], a safer alternative to cluster munitions [42], and intra-vehicular wireless LAN (WLAN). For the last application, consider the communication in a current mid-range civilian car. This car can contain over 50 sensors, with a wiring harness of 4000 parts, weighing 40 kg, with over 1900 wires, up to 4 km of wiring, and can be very costly [43]. A tank or other military combat vehicle has many times these levels. An intra-vehicle WLAN can significantly reduce this complexity, weight, and cost, and can reduce installation, upgrade, and repair times and expedite the relocation of systems within the vehicle. Furthermore the massive bandwidths available at mm-wave frequencies and above ensures that frequency diversity will provide jam resistance and a zero-error rate throughout the WLAN, while enabling the replacement of flexible, mechanically weak interconnections with more reliable and lighter weight packaged integrated circuits [1], thereby increasing the survivability of the system if individual elements are rendered inoperable. Another example is the recent DARPA Hot Spots program [44], developing UAV and ground vehicle network "hot spots" for high data rate backhaul at 71–86 GHz. Again, covertness and jam-resistance as well as high capacity are paramount requirements.

E. SUMMARY

All of the applications described above require a WLAN or wireless link that is high capacity, covert and secure from external jamming and hacking. The threat is not only from reception of the communications and signals by an adversary, but from vulnerability introduced by the inherently open nature of a wireless LAN. In particular, robotic vehicles have proven vulnerable to external manipulation, not only of their communications, but through the wireless link with an adversary directing control of their navigation and flight control systems [45], [46].

III. OPPORTUNITIES TO EXPLOIT MM-WAVE FREQUENCIES

Communication at mm-wave frequencies has the capability of providing high bandwidth, enabling the very high data rates needed by command post and swarming applications, and, with array antennas enabling high directivity beam-steering, they provide significantly lower RF link path loss than available at lower frequencies. In particular, the array antennas compensate for the higher link loss at mm-wave frequencies due to the smaller effective aperture of a single antenna element, compared to an antenna element size at the lower frequencies of 1 to 3 GHz (e.g. typical cellular frequencies). The narrower beam widths from antenna arrays, and the available beam steering, offer lower probability of intercept (LPI), lower susceptibility to interference, and greater resistance to jamming and hacking (outside the beamwidth). A number of papers have reported experiments using the frequency region near 60 GHz, where the atmospheric absorption reaches a peak, thus providing an abrupt drop in the link coverage—this is ideal for covert operation. The exponential propagation loss, e.g. 15 dB/km at 60 GHz at sea-level, due to atmospheric absorption contrasts with the relatively slow decrease due to $1/R^2$ free space spreading, e.g. 1.7 dB/km at 5 km. This abrupt drop enables a fairly ''hard'' boundary between reasonable EM reception and where signals are well below the noise level. By tuning the operating frequency around the absorption peaks, a covert ''bubble'' can be tailored around an area of secure communications which can be adaptively modified to accommodate changes in headquarter or swarm configurations, or weather conditions in real time. The atmospheric attenuation peak that is most extreme can be found at 380 GHz enabling ''whisper radio'' networks [1], [8] that cannot radiate beyond a few centimeters or meters. This covertness comes at the cost of higher output powers and/or higher gain directional beams that combat atmospheric attenuation, which emphasizes the desirability for adaptive ''tuning'' of the frequency-dependent exponential decay factor.

A. PROPAGATION AND ANTENNAS (MM-WAVE MYTH BUSTING

Fig. 3 shows the frequency dependence of atmospheric absorption for a communications link. For frequencies below 50 GHz and between 70 GHz and 110 GHz, and in the absence of rain, the absorption is much less than 1 dB/km and can be ignored for practical calculations for link distances less than 5 km. In this case the Friis equation for free space path loss can be used to calculate received power in the link. For lossless antennas, the antenna gain is equal to the directivity [48], and the Friis equation can be written [1], [2], [49], [50]:

$$\frac{P_r}{P_t} = \left(\frac{1}{4\pi R^2}\right)(D_t)\left(\frac{\lambda^2 D_r}{4\pi}\right) \tag{1}$$

where P_r and P_t are the received and transmitted powers, R is the range of the link, λ is the wavelength of the signal, and D_r and D_t are the directivity of the receiving and transmitting antennas respectively. The first term in the equation is just the $1/R^2$ path loss, which is independent of frequency. The second term is the directivity of the transmit antenna, D_t. The third term in brackets is the effective aperture area of the receive antenna (A_{er}) written out in terms of the directivity of the receive antenna and λ [48], [50]. For reference, the directivity of a resonant half-wave dipole antenna is: $D = 1.643$ [48].

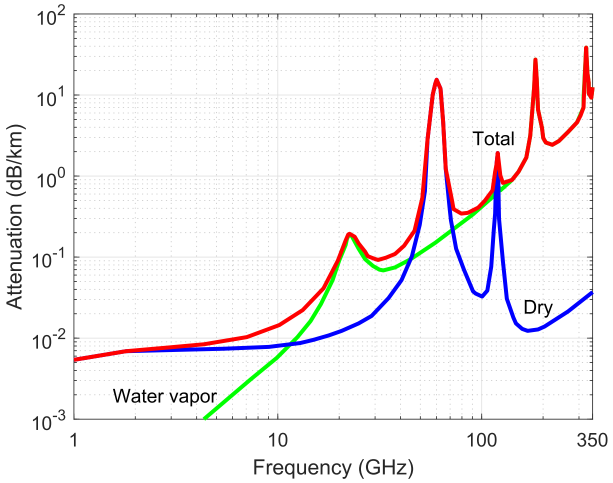


FIGURE 3. Specific atmospheric attenuation versus frequency [47]. Pressure = 1 atm = 101.325 kPa, temperature = 15°C, water vapor density = 7.5 g/m^3. Copyright International Telecommunications Union, used with permission.

TABLE 1. Frequency dependence of parameters relevant to the free space path loss for links between two resonant half-wave dipoles. N is the number of antenna elements at each end of the link.

f (GHz)	λ (cm)	N	D_t	D_r	A_e (cm^2)	Beam-width
6	5.00	1	1.64	1.64	3.26	360°
27	1.11	1	1.64	1.64	0.161	360°
39	0.769	1	1.64	1.64	0.0772	360°
72	0.417	1	1.64	1.64	0.0227	360°
141	0.213	1	1.64	1.64	0.00592	360°

For a link with single-element transmit and receive antennas, e.g. a resonant half-wave dipole antenna, the directivities are independent of frequency but both the physical sizes of the resonant dipoles, and the effective aperture of the antennas, and thus the received power, decrease with the square of frequency, see [1], [2], [48]. Table 1 shows the decrease in A_{er} of the receiving antenna as the frequency increases for a link with both transmit and receive antennas being half-wave resonant dipoles. The received power as a function of link range for a transmitted power of 1 W with half-wave dipole antennas is shown in the lower (a) curves in Fig. 4, and the noise floor for a practical receiver with a bandwidth of 1 GHz is also shown. (Ignoring processing gain and minimum SNR requirements, it is sufficient to consider that a signal can only be received if it exceeds the noise floor). The practical

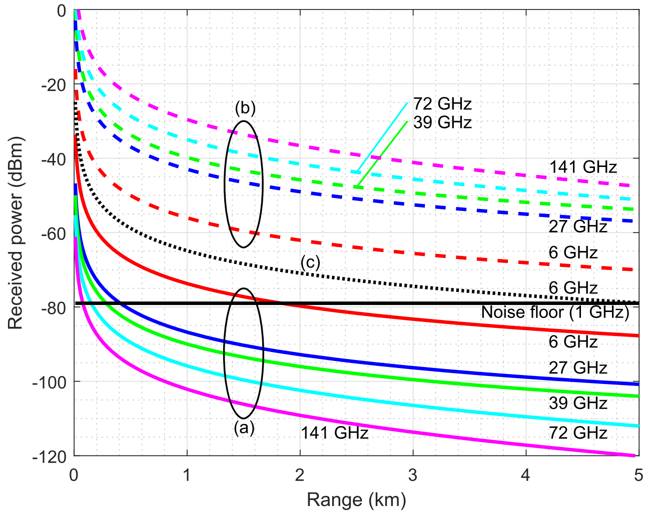


FIGURE 4. Received power for 1 W transmitted power between resonant half-wave dipole antennas ((a) curves), between two 5 cm × 5 cm antenna arrays of isotropic antenna elements spaced at half-wavelength separation ((b) curves), and between a resonant half-wave dipole and the same antenna array (curve (c)). The noise floor is calculated for a 1 GHz bandwidth using a thermal noise of −174 dBm/Hz plus a radio noise figure of 5 dB.

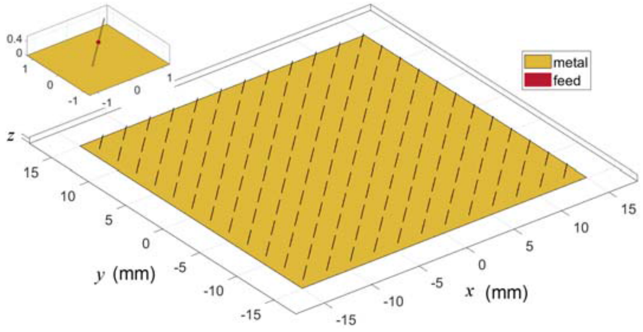


FIGURE 5. A 60 GHz 12 × 12 dipole array, with λ = 5 mm, on a λ/2 grid backed by a backplane reflector at a spacing of λ/10. Also shown is a unit element, a single dipole antenna with a backplane reflector with sides of dimension λ.

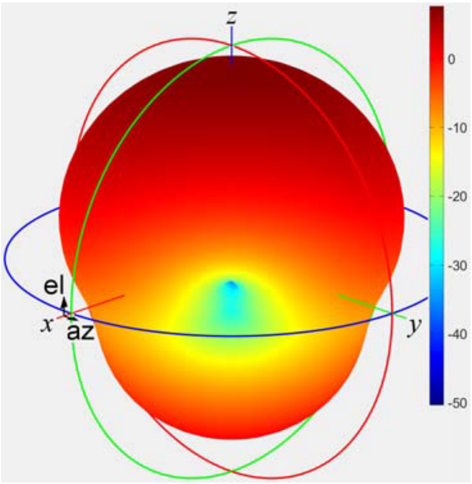


FIGURE 6. Field plot of the reflector-backed dipole antenna (see insert in Fig. 5) with a dBi scale. The directivity of the main lobe is 7 dBi. Note that the field wraps around the reflector.

transmission range at 72 GHz is limited to a very short distance, around 200 m, but reasonable transmission for a couple of kilometers is possible at 6 GHz. So, for single resonant half-wave dipole antennas, the higher mm-wave frequencies are not practical for LANs with link distances greater than a few hundred meters.

Most military platforms have a fixed (and constrained) physical area available for an antenna and at mm-wave frequencies the physical area available is sufficient for antenna arrays to be used. Using an antenna array increases transmit and receive directivity and with appropriate beam steering a link can be established between the transmit and receive antennas. The increase in directivity of an antenna array over the directivity of an individual antenna element is called array gain. For isotropic antenna elements arranged in a two-dimensional array spaced at $\lambda/2$ intervals, the directivity perpendicular to the plane of an array is (ignoring element-to-element coupling):

$$D = \pi A_p D_e / \lambda^2 \qquad (2)$$

where A_p is the physical area of the array which is equal to the effective aperture of the receiving array, and D_e is the directivity of a single antenna element. With an isotropic antenna element, which has $D_e = 1$, the entire directivity in (2) is then array gain. The array gain with other antenna elements is D/D_e increasing as the square of frequency (i.e. $1/\lambda^2$).

For a transmitter, an antenna array focuses energy in a particular direction thus reducing the possibility of detection. For a receiver, an antenna array concentrates the energy received from a particular direction and reduces the possibility of jamming. Here the antenna elements are considered as being lossless so that the directivity and antenna gain are the same. Consider the 60 GHz 12×12 array of reflector-backed dipole antennas in Fig. 5. The field plot of a single reflector-backed dipole antenna is shown in Fig. 6, where the z-directed main lobe has a directivity, i.e. antenna gain, of 7.7 dBi. (EM simulations were done using MATLAB® with the antenna toolbox.) This directivity compares to a free-standing dipole antenna which has an antenna gain of 1.8 dBi. This can be further compared to the focused field pattern of the array, see Fig. 7, with each element having the same drive where it is seen that the array has an antenna gain of 26.5 dBi. (This implies an array gain of 18.8 dB which is less than the theoretical array gain, from (2), of 21.2 dB and the short fall is attributed to element-to-element coupling.)

The array gain, i.e. increase in directivity, applies to both the transmit and receive antennas and (3) becomes [1]

$$\begin{aligned}\frac{P_r}{P_t} &= \left(\frac{1}{4\pi R^2}\right)\left(\frac{4\pi A_{pt} D_{et}}{\lambda^2}\right)\left(\frac{\lambda^2}{4\pi}\right)\left(\frac{4\pi A_{pr} D_{er}}{\lambda^2}\right)\\ &= \frac{A_{pt} D_{et} A_{pr} D_{er}}{R^2 \lambda^2}. \end{aligned} \qquad (3)$$

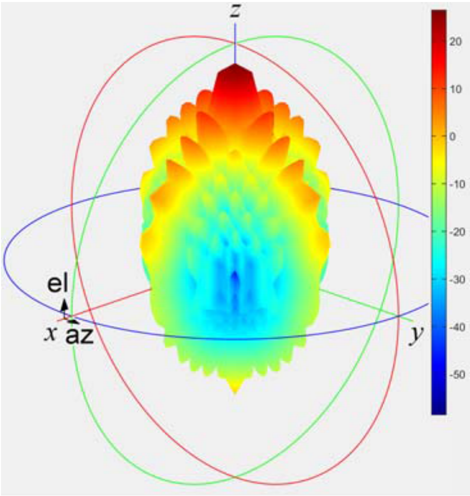


FIGURE 7. Field plot of the array in Fig. 5 with a dBi scale. The directivity of the main lobe is 26.5 dBi. The drive of each element has the same amplitude and phase.

TABLE 2. Frequency dependence of parameters relevant to the free space path loss for links between two square 5 cm × 5 cm arrays of isotropic antenna elements. The 3 dB beamwidth is calculated from [48].

f (GHz)	λ (cm)	N	D_t	D_r	A_e (cm^2)	Beam-width
6	5	4	12.6	12.6	25	52.6°
27	1.11	81	254	254	25	11.3°
39	0.769	169	531	531	25	7.82°
72	0.417	576	1810	1810	25	4.23°
141	0.213	2209	6940	6940	25	2.16°

Here A_{pt} and A_{pr} are the physical sizes of the transmit and receive antenna arrays, and D_{et} and D_{er} are the antenna gains of the individual transmit and receive antenna elements, respectively. Now, for the system with antenna arrays at both the transmitter and receiver, the λ^2 dependence of the received power for single elements, see (1), is *inverted* to a $1/\lambda^2$ dependence so that the receive power increases as the square of frequency. As shown in Table 2, as the frequency increases, for a fixed physical array size, the number of antenna elements in each array increases (as the square of the frequency), and the directivities increase while the beamwidths of the main antenna lobes decrease proportionately as the effective aperture remains independent of frequency.

As an example, with transmit and receive arrays having a physical size of 5 cm × 5 cm, isotropic antenna elements spaced at $\lambda/2$ separations, and with 1 W transmitted power, the received powers at different frequencies are shown in the upper (b) curves of Fig. 4. While neglecting weather and atmospheric effects, clearly there is a significant propagation advantage to operating at higher mm-wave frequencies. Not only do the array antenna curves show much less RF link path loss than the paired dipole antenna curves, but the order of the curves is "flipped," with the higher frequency arrays delivering higher signal powers than the lower frequency arrays. This analysis assumes optimum coupling to the antennas, low resistive loss in the antennas, optimum pointing, and optimum polarization coupling to the antennas, but any specific antenna configuration will have the same $1/\lambda^2$ propagation dependence [1]. For now, atmospheric absorption has been ignored but this will be a multiplicative factor that will be considered later.

In some network configurations it may be useful to have links between omni-directional dipole antennas and array antennas, e.g. for links between handheld devices and base stations [2]. In this case the free space path loss equation shows no dependence for frequencies below 52 GHz, between 70 GHz and 110 GHz, and a narrow band near 140 GHz. Curve (c) in Fig. 4 illustrates the received power for a transmitted 1 W signal and shows it to provide reasonable propagation for links below 5 km. Note the slow roll off in power of the $1/R^2$ part of the function (i.e. higher R). Combined with the low path loss and higher bandwidth at higher mm-wave frequencies, this slow roll off would argue that the higher mm-wave frequencies could be useful for back haul over modest distances as well as for intra-WLAN communications.

B. ATMOSPHERIC ABSORPTION SECURITY BUBBLE

A relatively slow roll off of received power with distance can present problems with network security, where a signal strong enough to provide assured high data rate communications will be subject to detection, jamming, and hacking from well outside the WLAN. To mitigate this vulnerability, the frequency regions of high atmospheric absorption can be exploited. For example, the higher absorption between 50 GHz and 70 GHz is due primarily to atmospheric oxygen absorption, which peaks at 60 GHz. This relatively steep absorption line yields an exponential increase of link loss with distance and provides an opportunity to tune a "security bubble" around the links in the network, with good communications within the bubble and virtually undetectable and uninterruptable communications a few kilometers outside the bubble. Fig. 8 illustrates the tuning of the RF link path loss by adaptively tuning the frequency to achieve different sizes of security bubbles around a link and to accommodate different environmental conditions.

The atmospheric absorption shown in Fig. 3 is valid for sea level. For the high altitudes of aircraft WLAN's or UAV swarms, the atmospheric absorption is reduced and becomes much more complex, as shown in Fig. 9. In some bands, e.g. around 60, 118, 183, and 323 and 380 GHz [5], [8], adaptive tuning can now be used to achieve enhanced security.

There is a loss (or power) trade-off for leveraging the absorption security bubble. At the maximum covertness (say at 60 GHz), the loss is about 15 dB/km. This is partially offset by the 20 dB directivity advantage compared with operating at 6 GHz with the same physical size aperture. For practical operation, the operator will need the ability to tune the size of the security bubble (and therefore link loss) by tuning frequency to balance the needed covertness with power loss. Automatic adaptivity may be engineered into the network

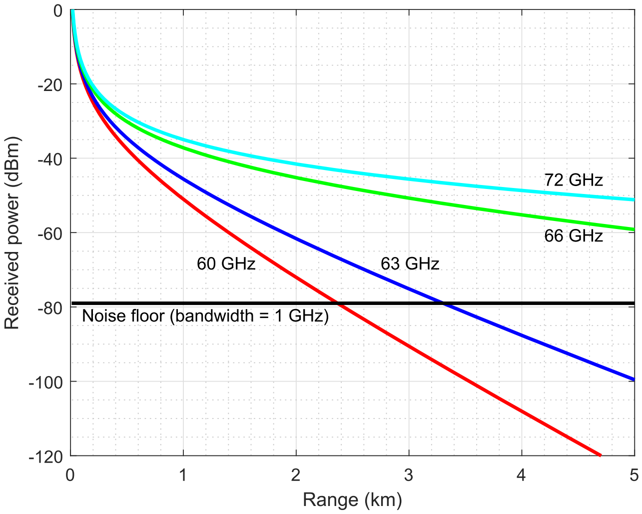


FIGURE 8. Received link power for 1 W transmitted between the antenna arrays described in Fig. 4 in the frequency range of high atmospheric absorption.

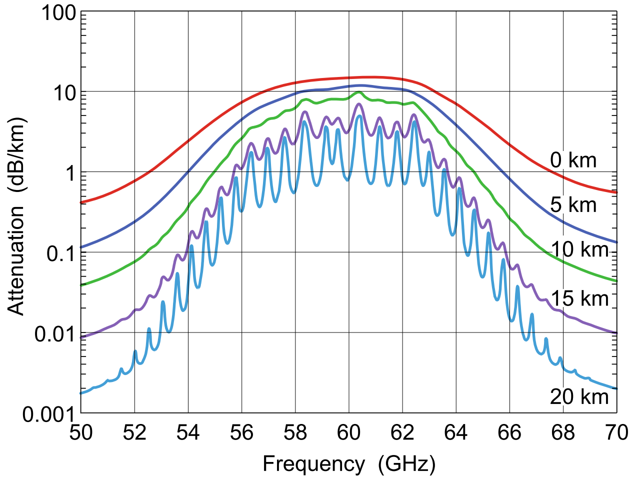


FIGURE 9. Specific atmospheric absorption around 60 GHz at different altitudes above sea-level. After [47]. Copyright International Telecommunications Union, used with permission.

circuitry to manage this trade-off in real time for changing link distances, security requirements, and environmental conditions.

The coverage of a communications signal will be affected by rain. For example the scattering loss due to heavy rain (50 mm/hour) is 1 dB/km at 10 GHz, 10 dB/km at 30 GHz, and increasing to 20 dB/km at 90 GHz where it begins to flatten out at greater frequencies [2]. Thus at 5 km distance, the additional attenuation is only 5 dB at 10 GHz, but 100 dB at 90 GHz. The 5 dB of loss at 10 GHz can easily be compensated by increasing the transmitted power by 5 dB, or by using a larger physical antenna aperture at one end of the link, but it is unreasonable to expect that the transmit power at 90 GHz can be increased by 100 dB to maintain the RF link over 5 km. From a system design perspective this means that the communications link must be able to switch operation among a number of bands, as well as being able to be adaptive over a narrower range around those bands. However, the rain ensures some covertness above 10 GHz. This means that operation at 10 GHz becomes reasonable in rain, even though directivity is significantly less than at the mm-wave frequencies.

C. CIRCUIT COMPLEXITY

The analysis so far has focused on the propagation opportunities provided by higher mm-wave frequencies for WLAN architectures. In order to effectively exploit the advantages, the electronics at each network node will become substantially more complicated to accommodate the tracking and pointing requirements of the directional links and the adaptive tuning within the absorption lines. Additional complexity may be needed to accommodate high bandwidth communications where the received power is highly frequency dependent. Recent and current mm-wave circuit development has been greatly energized by the requirement to support the new 5G commercial networks. These developments will be leveraged for military applications.

While the pointing and tracking functions will be more critical for the array, the increased requirement will not be excessive. For example, even at 141 GHz, the beam width is 2.16° in our previous example (see Table 2) so that at 1 km link distance the 3 dB beam span is 38 m. At shorter link distances, for example at 100 m link range, the beamwidth can be electronically spread by phasing individual antenna elements to maintain the same 38 m beam width.

IV. CONCLUSION

Two major conclusions derive from this paper. First, we showed that the higher mm-wave frequencies provide significantly better path loss conditions for network links in a field command post or robotic swarm, where the antenna apertures are constrained by a fixed area so that antenna arrays can be used. Second, the mm-wave region between 50 GHz and 70 GHz (and at higher frequency mm-wave bands) provides an opportunity to adaptively tune the covertness and vulnerability (or potential to interfere with nearby networks) of the network, which will also be useful for a number of other military wireless applications. These conclusions need to be incorporated in the concept development and engineering of new military communications networks.

Disclaimer: In composing this article, the authors relied solely on information in the public domain. It was not based on any special knowledge of military systems. It does not represent the official position or programs of the US Department of Defense.

REFERENCES

[1] T. S. Rappaport, R. W. Heath, Jr., R. C. Daniels, and J. N. Murdock, *Millimeter Wave Wireless Communications*. London, U.K.: Pearson Education, 2014.

[2] Y. Xing and T. S. Rappaport. (2018). "Propagation measurement system and approach at 140 GHz-moving to 6G and above 100 GHz." [Online]. Available: https://arxiv.org/abs/1808.07594

[3] T. S. Rappaport, G. R. Maccartney, M. K. Samimi, and S. Sun, "Wideband millimeter-wave propagation measurements and channel models for future wireless communication system design," *IEEE Trans. Commun.*, vol. 63, no. 9, pp. 3029–3056, Sep. 2015.

[4] R. C. Daniels, J. N. Murdock, T. S. Rappaport, and R. W. Heath, Jr., "60 GHz wireless: Up close and personal," *IEEE Microw. Mag.*, vol. 11, no. 7, pp. 44–50, Dec. 2010.

[5] T. S. Rappaport *et al.*, "Millimeter wave mobile communications for 5G cellular: It will work!" *IEEE Access*, vol. 1, pp. 335–349, May 2013.

[6] A. Bleicher, "The 5G phone future," *IEEE Spectr.*, vol. 50, no. 7, pp. 15–16, Jul. 2013.

[7] S. L. Cotton, W. G. Scanlon, and B. K. Madahar, "Millimeter-wave soldier-to-soldier communications for covert battlefield operations," *IEEE Commun. Mag.*, vol. 47, no. 10, pp. 72–81, Oct. 2009.

[8] T. S. Rappaport, J. N. Murdock, and F. Gutierrez, Jr., "State of the art in 60-GHz integrated circuits and systems for wireless communications," *Proc. IEEE*, vol. 99, no. 8, pp. 1390–1436, Aug. 2011.

[9] P. Scharre, "Robotics on the battlefield part II, the coming swarm," *Center New Amer. Secur.*, pp. 1–61, Oct. 2014.

[10] C. Lombardo and K. Selby, "Iron brigade's combat-team pursuit of mobile command-post capabilities," *Armor*, vol. 128, no. 3, pp. 57–61, 2017. [Online]. Available: http://www.benning.army.mil/armor/eARMOR/content/issues/2017/Summer/pdf/ARMOR_Summer_2017_edition.pdf

[11] F. Clemente and S. Gray, "The future of the command post: Artificial intelligence could turn data paralysis into information analysis," *Signal Mag.*, p. 29, Oct. 2018.

[12] A. Stone, "Army building the command post of the future," *Armor*, vol. 128, pp. 57–61, Aug. 2016. [Online]. Available: https://www.c4isrnet.com/it-networks/2016/08/17/army-building-command-post-of-the-future/

[13] USSOCOM, "Capability production document for united states special operations command (USSOCOM) tactical local area network (taclan)," *Armor*, vol. 128, p. 11, Mar. 2004. [Online]. Available: https://www.socom.mil/FOIA/FOIA%20Contracts/H92222-05-D-0017/Attachments/Attachment%203.pdf

[14] S. J. Freeman, Jr., "Miserable, disobedient and victorious: General milley's future US soldier," in *Breaking Defense*, M. Milley, Ed. Arlington, VA, USA: Association of the United States Army, Oct. 2016. [Online]. Available: https://breakingdefense.com/2016/10/miserable-disobedient-victorious-gen-milleys-future-us-soldier/

[15] A. Stone. (Jan. 14, 2016).*Army Makes Big Leap in Command Post Wi-Fi-C4ISRNET*. [Online]. Available: https://www.c4isrnet.com/it-networks/2016/01/14/army-makes-big-leap-in-command-post-wi-fi/

[16] D. Lafontaine. (Jan. 10, 2018). *Army Launches Effort to Integrate Command Post Components*. [Online]. Available: https://www.army.mil/article/198943/army_launches_effort_to_integrate_command_post_components

[17] N. R. Augustine, *Augustine's Laws and Major System Development Programs*. Reston, VA, USA: American Institute of Aeronautics and Astronautics, 1983.

[18] F. W. Lanchester, "Mathematics in warfare," in *The World of Mathematics*, vol. 4, J. R. Newman, Ed. Simon and Schuster, 1956, pp. 2138–2157.

[19] *Lanchester's Laws*. Accessed: Apr. 22, 2019. [Online]. Available: https://en.wikipedia.org/wiki/Lanchester%27s_laws

[20] D. A. Shlapak, D. T. Orletsky, T. I. Reid, M. S. Tanner, and B. Wilson, *A Question of Balance: Political Context and Military Aspects of the China-Taiwan Dispute*. Santa Monica, CA, USA: Rand Corporation, 2009. [Online]. Available: http://www.rand.org/pubs/monographs/MG888.html

[21] NASA Technology Transfer Program, Washington, DC, USA. *Autonomous Positioning and Navigation Network*. Accessed: Apr. 22, 2019. [Online]. Available: https://ntts-prod.s3.amazonaws.com/t2p/prod/t2media/tops/pdf/MFS-TOPS-64.pdf

[22] J. Trevithick. (Dec. 29, 2017). *USAF Wants Swarms of Cheap 'Gray Wolf,' Cruise Missiles that can Overwhelm Enemy Defenses*. [Online]. Available: http://www.thedrive.com/the-war-zone/17257/usaf-wants-swarms-of-cheap-gray-wolf-cruise-missiles-that-can-overwhelm-enemy-defenses

[23] (Jan. 16, 2018). *China is Hard at Work Developing Swarms of Small Drones With Big Military Applications*. [Online]. Available: http://www.thedrive.com/the-war-zone/17698/chinas-is-hard-at-work-developing-swarms-of-small-drones-on-multiple-levels.

[24] A. Harper. (Nov. 16, 2018). *Drones Level the Battlefield for Extremists*. [Online]. Available: https://www.lowyinstitute.org/the-interpreter/drones-level-battlefield-extremists

[25] A. Tate. (Jun. 22, 2017). *China Launches Record-Breaking UAV swarm*. [Online]. Available: https://www.realcleardefense.com/2017/06/22/china_launches_record-breaking_uav_swarm_294247.html

[26] H. Williams, "KB radar develops UAV-based satcom and navigation jammers," *IHS Jane's Int. Defence Rev.*, p. 29, Oct. 2016.

[27] H. Williams, "UAS focus should shift to mission suites," *IHS Jane's Int. Defence Rev.*, p. 25, Sep. 2016.

[28] P. Tucker. (2017). *Drones Will Help Protect Guam From North Korean Missiles*. [Online]. Available: https://www.defenseone.com/technology/2017/08/drones-will-help-protect-guam-north-korean-missiles/140400/

[29] I. Lachow, "The upside and downside of swarming drones," *Bull. Atomic Sci.*, vol. 73, no. 2, pp. 96–101, 2017. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/00963402.2017.1290879

[30] J. Spencer. (Dec. 11, 2017). *How Drone Swarms Could Change Urban Warfare-C4ISRNET*. [Online]. Available: https://www.c4isrnet.com/opinion/the-compass/net-defense-blogs/2017/12/11/how-drone-swarms-could-change-urban-warfare-commentary/

[31] G. Jennings, "US demonstrates one of the world's largest micro-UAV swarms," *IHS Jane's Defence Weekly*, p. 12, Jan. 2017.

[32] M. Pomerleau. (Oct. 26 2016). *Navy Outlines Path Forward on Unmanned Systems-C4ISRNET*. [Online]. Available: https://www.c4isrnet.com/unmanned/uas/2016/10/26/navy-outlines-a-path-forward-on-unmanned-systems/

[33] (Jul. 26, 2016). *Navy Taking Domain-Agnostic Approach to Unmanned Systems-C4ISRNET*. [Online]. Available: https://www.c4isrnet.com/unmanned/uas/2016/07/26/navy-taking-domain-agnostic-approach-to-unmanned-systems

[34] M. Melenic, "Lockheed Martin conducts UAV launch from UUV," *IHS Jane's Int. Defence Review*, p. 14, Nov. 2016.

[35] S. Gorman, Y. J. Dreazen, and A. Cole, "Insurgents hack U.S. drones," *Wall Street J.*, vol. 263, p. 1, Dec. 2009.

[36] R. Boland. Mar. 2010. *Simulation Project Demonstrates Covert Application*. [Online]. Available: https:www.afcea.org/content/?q=simulation-project-demonstrates-covert-applications/

[37] G. Fein, "Hands-free resupply: US Army moves closer to setting requirements for JTARV," *IHS Jane's Int. Defence Rev.*, pp. 28–29, May 2016.

[38] P. McLeary. (Aug. 23, 2018). *Special OPS Command to Hold Flyoff of Tiny Drones*. [Online]. Available: https://breakingdefense.com/2018/08/special-ops-command-to-hold-flyoff-of-tiny-drones/

[39] M. S. Heimbeck and D. de Ceglia, "Resonant inductive power transfer for noncontact launcher-missile interface," AMRDEC, Huntsville, AL, USA, Tech. Rep. RDMR-WD-16-37, Aug. 2016. [Online]. Available: https://www.dtic.mil/dtic/tr/fulltext/u2/1013776.pdf

[40] G. Fein, "US Army advances robotic wingman concept," *IHS Jane's Int. Defence Rev.*, p. 23, May 2017.

[41] H. Williams, "Unmanned and unguarded: Operators and industry look to close a defence gap—UAS survivability," *IHS Jane's Int. Defence Rev.*, pp. 50–55, May 2017.

[42] D. Wasserby, "Cluster munitions: The US aims for safer submunitions with the same effects," *IHS Jane's Int. Defence Rev.*, pp. 60–65, Jul. 2018.

[43] M. Ahmed, C. U. Saraydar, T. ElBatt, J. Yin, T. Talty, and M. Ames, "Intra-vehicular wireless networks," in *Proc. IEEE Globecom Workshops*, Nov. 2007, pp. 1–9.

[44] H. B. Wallace, "DARPA mmw system programs and how they drive technology needs," in *Proc. DMRC Millimeter-Wave Technol. Workshop*, Oct. 2014, pp. 1–25. [Online]. Available: https://www.ece.ucdavis.edu/dmrc/files/2014/09/Bruce_wallace_darpa_web.pdf

[45] C. Mortimer. (Nov. 21, 2017). *Hackers Now Able to Take Control of Cars to Cause Deliberate Accidents, Scientists Warn*. [Online]. Available: https://www.independent.co.uk/life-style/gadgets-and-tech/news/computer-hackers-control-car-deliberate-accidents-national-security-issue-a8066466.html

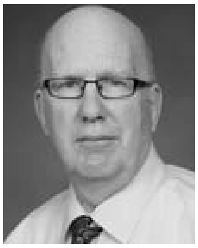
[46] M. D. Cava. (Jun. 6, 2016). *Mitsubishi Outlander Hacked Through in-Car WiFi*. [Online]. Available: https://www.usatoday.com/story/tech/news/2016/06/06/mitsubishi-outlander-hacked-through–car-wifi/85499390/

[47] *Attenuation by Atmospheric Gases*, document Recommendation ITU-R P.676-11, Sep. 2016.

[48] C. A. Balanis, *Antenna Theory: Analysis and Design*. Hoboken, NJ, USA: Wiley, 2016.

[49] H. T. Friis, "A note on a simple transmission formula," *Proc. IRE*, vol. 34, no. 5, pp. 254–256, May 1946.

[50] T. S. Rappaport, *Wireless Communications: Principles and Practice*, vol. 2. Upper Saddle River, NJ, USA: Prentice-Hall, 1996.



JAMES F. HARVEY received the B.S. degree in engineering from the U.S. Military Academy, the M.A. degree in physics from the Dartmouth College, and the Ph.D. degree in applied science from the University of California, Davis. He is currently a Research Program Manager for the Electronics Division Program on Bio-Electronics and Nano-Electronics with the U.S. Army Research Office. He also provides program assistance to the OSD Basic Research Office for the Multidisciplinary University Research Initiative (MURI), Defense University Research Instrumentation Program (DURIP), and the OSD Pilot Program: Innovation Corps @ Department of Defense (I Corps@DoD). His previous research interests include electromagnetics, microwave circuit engineering, and laser plasmas.

MICHAEL B. STEER joined as the Jack S. Kilby Lecturer, in 2003. He is currently the Lampe Distinguished Professor of electrical and computer engineering with North Carolina State University (NC State). He has authored more than 500 refereed publications and four books. He was a member of the MTT-S Administrative Committee, from 1998 to 2001, from 2003 to 2006, and from 2016 to 2018. He was a recipient of the Presidential Young Investigator Award, in 1986, the Army Medal, in 2009, the Commander's Award for Public Service, in 2009, and the 2010 Microwave Prize for the Best Paper on Microwave Engineering in any IEEE publication in the preceding year. He received the Service Recognition Award from the society, in 1998 and 2001, the Alcoa Foundation Distinguished Research Award from the NC State's College of Engineering, in 2003, the Bronze Medallion from the U.S. Army Research for Outstanding Scientific Accomplishment, in 1994 and 1996, the Distinguished Service Recognition Award from IEEE MTT-S, in 2007, the Distinguished Educator Award from IEEE/MTT-S, in 2011, and the R.J. Reynolds Award for Excellence in Teaching, Research, and Extension from the College of Engineering, NC State University, in 2013. He received the Alexander Quarles Holladay Medal from NC State University, in 2017. This is the highest award made by the university in recognition of faculty career achievements. In 2010 he was inducted into the Electronic Warfare Technology Hall of Fame sponsored by the Association of Old Crows and was named as one of the Most Creative Teachers in the South by *Oxford American Magazine*. He has led three Multidisciplinary University Research Innovation (MURI) projects which are large projects funded by the U.S. Department of Defense and involve multiple universities. He was a Secretary of the IEEE Microwave Theory and Techniques Society (MTT-S), in 1997. He was the Editor-in-Chief of the IEEE TRANSACTIONS ON MICROWAVE THEORY AND TECHNIQUES.

THEODORE S. (TED) RAPPAPORT received the Ph.D. degree from Purdue University, in 1987.

His Ph.D. study provided fundamental knowledge of indoor wireless channels and was used to create the first Wi-Fi standard (IEEE 802.11). He founded three academic wireless research centers at Virginia Tech, The University of Texas, and NYU that have produced thousands of engineers and educators, since 1990. He co-founded two wireless companies, TSR Technologies and Wireless Valley Communication, which were sold to publicly traded companies and has advised many others. He co-founded the Virginia Tech Summer School and Wireless Symposium, in 1991, the Texas Wireless Summit, in 2003, and the Brooklyn 5G Summit (B5GS), in 2014. He is currently the David Lee/Ernst Weber Professor with New York University (NYU), where he holds faculty appointments with the Electrical and Computer Engineering Department, NYU Tandon School of Engineering; the Courant Computer Science Department; and the NYU Langone School of Medicine. He is the Founder and the Director of NYU WIRELESS, a multidisciplinary research center focused on the future of wireless communications and applications. His research has led the way for modern wireless communication systems. He conducted fundamental work that led to the first U.S. Digital cellphone standards, TDMA IS-54/IS-136 and CDMA IS-95. He and his students engineered the world's first public Wi-Fi hotspots, and more recently, his work proved the viability of millimeter waves for mobile communications. The global wireless industry adopted his vision for fifth-generation (5G) cellphone networks. He has coauthored over 300 papers and 20 books, including the most cited books on wireless communications, adaptive antennas, wireless simulation, and millimeter-wave communications. He holds more than 100 patents.

He is a Fellow of the Radio Club of America and the National Academy of Inventors, and a Life Member of the American Radio Relay League. He was a recipient of the ASEE's Terman Award, the IEEE Education Society William E. Sayle Award for achievement in education, and the IEEE Communications Society Armstrong Award. He received the Sir Monty Finniston Medal from the Institution of Engineering and Technology (IET), the IEEE Vehicular Technology Society's James R. Evans Avant Garde Award and the Stu Meyer Award, and the Armstrong Medal from the Radio Club of America. He is a Licensed Professional Engineer in Texas and Virginia, and an Amateur Radio Operator (N9NB). He has served for the Technological Advisory Council of the Federal Communications Commission (FCC).

• • •