Impact of an intelligent jammer on the emergency services’ communication system

Ray R. Tanuhardja
M.Sc. Thesis
19 December 2013

Supervisors:
prof. dr. ir. Ing. F.B.J. Leferink
dr. ir. M.J. Bentum
dr. ir. G.J. Heijenk
G.S. van de Beek M.Sc.

Telecommunication Engineering Group
Faculty of Electrical Engineering, Mathematics and Computer Science
University of Twente
P.O. Box 217
7500 AE Enschede
The Netherlands
Impact of an intelligent jammer on the emergency services’ communication system

R.R. Tanuhardja
Department of Electrical Engineering, Faculty of EEMCS, University of Twente
Drienerlo 5, 7522 NB Enschede, The Netherlands
Email: r.r.tanuhardja@student.utwente.nl

Abstract—C2000 is a communication system based on the Terrestrial Trunked Radio (TETRA) protocol and is used in the Netherlands by emergency services. We investigated the resilience of the voice component of C2000 against intelligent intentional electromagnetic interference (IEMI). Low power signals interfering with the system’s higher protocols have the advantage of staying covert. The analysis shows that if the access assignment channel is corrupted, the mobile stations cannot start conversations with the base station. TETRA’s modulation scheme is also investigated. \( \pi/4 \) Differential Quaternary Phase Shift Keying (DQPSK) is interfered with a continuous wave and a Quaternary Phase Shift Keying (QPSK) signal. The results show that a continuous wave created the largest error vector magnitude (EVM), but creates a peak in the received spectrum. The power of the QPSK signal, however, is distributed over a bandwidth and is more difficult to detect than the continuous wave in the received spectrum. From this we conclude that the QPSK signal functions better as an intelligent interference signal compared to the continuous wave. In this thesis it is shown that it is possible to create a jammer that combines the vulnerability in the TETRA protocol with the QPSK signal to disrupt the communication system, while staying covert. This can cause dangerous situations during large calamities, but also during small felonies where adversaries can disrupt the communication locally.

Index Terms—C2000, TETRA, intelligent jammer, IEMI, emergency services, communication system

I. INTRODUCTION

In 2004 the C2000 wireless digital communication system replaced the previous analogue system in the Netherlands [1]. Advantages of the modern private mobile radio (PMR) system over the previous analogue PMR system are the utilisation of data communication, the robustness, and the encryption of traffic [2]. Furthermore, C2000 was designed in such a way that the different emergency services sections could communicate with each other, e.g., ambulance personal can communicate with the fire brigade using this communication system. Communication between emergency services is very important to be able to cope with emergencies. The outcomes can lead to disasters if the communication is not working properly as was the case in the air plane crash of Turkish Airlines flight 1951, the riots on the beach of Hoek van Holland, and the Project X incident in Haren in October 2012 [3]–[6]. The design of the system also causes to lose communication with firemen completely if they enter buildings and the signal drops below a certain threshold level [7]. These examples show that the outcomes can be quite severe if the communication system is down.

These problems occurred without the intention of malevolent actions, but it is very interesting to what extent the system is able to resist intentional attacks. Terrorist attacks can create much more devastation if they are able to interfere with the communications especially if the IEMI is covert. By recognising the possible vulnerabilities it is possible to take adequate counter measures and increase the security of the system. C2000 consists of a paging system, a voice communication component, and some extra functional additions specifically for the Netherlands [1]. This thesis will limit itself to the voice communication component, called T2000, which is based on the Terrestrial Trunked Radio protocol (TETRA) [1]. Once the voice communication is down, then the main functionality of the system is gone and the communication system is successfully disrupted. Wireless communication systems, such as C2000, are especially sensitive to attacks from adversaries, since the nature of the medium is shared and easy to access [8]. Electromagnetic interference (EMI) can be created unintentionally. In this thesis, however, the focus is on jammers, which are devices that create intentional electromagnetic interference (IEMI) to deliberately damage systems or deny users of service. There are several examples of jammers that are commercially available that interfere with other wireless communication systems [9]–[11].

IEMI attacks can be divided in two large categories: back door coupling attacks and front door coupling attacks. Back doors are coupling paths that are not designed to receive signals and front doors are coupling paths that are designed to receive signals, e.g., antennas. The coupled power falls off strongly outside the bandwidth the antenna is designed for [12]. Therefore, to achieve maximum impact with a front door coupling attack, a priori knowledge of the victim’s frequencies is required to interfere the communications. It is possible to use either high power or low power IEMI attacks. High power attacks create electromagnetic fields with very high amplitudes to damage or upset the victim’s system [13], [14]. High power attacks can be via both back door and front door, while low power IEMI attacks are most often via the front door where they interfere with signals.

Although high power IEMI attacks can damage the low noise amplifiers of the receiver modules, random high power IEMI attacks via the front door are not as effective at damaging the RF power amplifiers of the sending modules as shown in [14]. They show that digital modulation schemes are much more sensitive than the RF power amplifiers, if the interference...
signal are in the bandwidth of the intended received modulated signals. This work focusses on low power IEMI attacks via the front door to interfere with the modulation scheme used by TETRA. The first advantage is that low power intelligent attacks are more likely to stay covert. This makes it hard for systems to detect and to respond to these kinds of attacks. Second, less power is required. In addition, high power wideband systems are usually large systems [13]. The impact area of high power IEMI attacks via the backdoor are currently limited to approximately one kilometre [15]. Low power IEMI attacks have a larger range since high power field strengths are not necessary. They are not aimed at damaging the hardware, but at interfering with the control signals. Furthermore, low power intelligent IEMI focusses only on the systems under attack.

There are several low power IEMI jammers possible: constant jammers, deceptive jammers, random jammers, reactive jammers, and intelligent jammers [16]. More information about the first four jammers can be found in [8], [16], [17]. This thesis focusses on intelligent low power jammers, which exploit weaknesses in higher protocols to impair the correct functioning of the communication system with very low energy jamming and deny users of service. These jammers require extensive information of the victim’s protocol and are more complex.

Smart jamming attacks on wireless systems have already been investigated. Jamming attacks focussing on the synchronisation procedures of the GSM network can successfully deny mobile terminals of service [18]. There are even more smart jamming attacks focussing on the IEEE 802.11 protocol. Corrupting the Clear to Send messages and Acknowledgement messages are just two examples of the many possibilities to disrupt the IEEE 802.11 protocol in an intelligent way. An extensive overview is given in [8]. Although, TETRA has been tested with Additive White Gaussian Noise, smart jamming attacks focussing specifically on TETRA have not yet been investigated. Therefore, it is still unknown whether adversaries are able to compromise the system. As stated before, this communication system is especially critical since failing of the system can result in disastrous outcomes of emergencies.

Therefore the aim of this thesis is to investigate the resilience of TETRA against intelligent intentional electromagnetic interference. Low power IEMI will be used to interfere with the higher protocols. A closer look at the modulation at the physical layer will be taken and it is analysed how the modulation scheme can be interfered with.

In Section II an overview of the TETRA system is given to get familiar with the protocol. The vulnerabilities are highlighted and the effect of a QPSK modulated and continuous wave as interference signals on the digital modulation scheme used by TETRA is investigated. Using this analysis, a jammer is then described that is able to impair the communications between the mobile station and base station. In Section III experiments to verify the effect of the interference signal on the modulation scheme are described. In Section IV, the results of the superposition of the digital modulation schemes are shown. The results are discussed in Section V. Conclusions are drawn in Section VI. Finally, recommendations for future work are suggested.

II. Analysis

Intelligent jammers are devices which exploit higher layer protocols to interfere with a communication system. Therefore, a lot of prior knowledge of the system is required. First an overview of TETRA is given to get familiar with the protocol. Second, vulnerabilities are exposed. Third, interference with the modulation scheme is investigated. The aim is to find a difficult to detect signal with a small amplitude. These signals are simulated in Simulink [19] to determine which are best to obtain a high bit error rate. Finally, by combining the acquired knowledge of the vulnerabilities and the interference signal, a jammer is proposed to successfully interfere with the TETRA system.

A. Overview TETRA

The specifications for TETRA is defined by the European Telecommunications Standards Institute (ETSI). TETRA is a digital mobile communication standard for PMR. The basic services TETRA provides are data communications, encryption of traffic, voice calls to individual mobiles, groups calls, and broadcast calls [20]. An overview of the main physical layer parameters is shown in Table I.

TETRA works in trunked mode operation with a base station and direct-mode operation between mobiles. In direct-mode operation the mobile stations communicate directly with each other. Since there is no base station in this operation, a special procedure is followed for synchronisation between these devices [21]. This thesis focusses itself to the trunked mode circuit switching operation with a base station. If this part of the system is disrupted, then the emergency services on location cannot call for backup. Furthermore, the location of the base station is known and therefore it is easier to estimate the demands to interfere with the signals of the base station.

TETRA is a cellular network and every cell in this kind of network has its own base station [21]. Each cell is provided with a number of channels which can be used for traffic and signalling. A communication link between mobiles and a base station is made in trunked mode operation. The base stations are connected to a mobile switching centre, which are connected to the rest of the network.

The use of a cellular radio system poses some challenges. Like every radio system, the amount of spectrum available is fixed. Wireless communication with radio waves has the usual issues like multipath propagation, fading, and interference. Furthermore, the cellular concept poses another challenge. The mobile can move between different cells, which implies that the link between the mobile and base station has to be transferred to the new cell’s base station. This transferring between cells is handled by a process called ‘handover’. There are more challenges for cellular networks (summarised in [21]), but not relevant for this research.

C2000 is based on TETRA and the security has improved substantially compared to the previous emergency services communication system. Authentication and confidentiality are both implemented in TETRA [20]. All TETRA equipment has a unique number to identify themselves with the network called a TETRA Equipment Identity (TEI). This is a 60 bit
long number. Once a mobile device has been identified, the network can decide to disable or deny the mobile of service if its TEI is noted as stolen or obsolete. Furthermore, the mobile terminal can be monitored with some operational or security checks before the link is shut down. These things make it hard to spoof the network with a false number. Authentication is based on this unique number. Confidentiality is achieved via air-interface encryption and end-to-end encryption. The air-interface encryption is achieved in the data link layer, while the end-to-end encryption is embedded in the higher application layers.

TETRA is defined for the first three layers; physical layer, data link layer, and the network layer; of the Open Systems Interconnection model (OSI model) [2], [20], [21]. In this thesis the focus is mainly on the physical layer, because at this layer the physical signals are interfered with. If this layer does not function properly the layers above also cannot function well.

In the physical layer, the bits are sent via radio waves from the mobile station to the base station and vice versa. TETRA can operate in the bandwidth of 150 MHz to 900 MHz, but the C2000 system is limited to 380 to 395 MHz in the Netherlands [22]. The carrier spacing is 25 kHz. However, to make optimal use of the limited allocated bandwidth, the TETRA system also uses 4 slots time division multiple access (TDMA). Each burst of information is transmitted in one slot. For the digital modulation TETRA uses $\pi/4$-Differential Quaternary Phase Shift Keying ($\pi/4$-DQPSK). The phase transitions of this modulation type is shown in Figure 1 and Table II. The modulation switches between the two constellation diagrams as shown in Figure 2. The advantages of using this modulation type is that there is no need for an exact synchronised phase reference signal at the receiver and the signal does not pass through the origin. This means that the amplitude of the signal does not go to zero, which puts less constraints on the linearity of the power amplifier of the transmitter. The dibit is reproduced by comparing the current phase with the previous phase. Furthermore, the maximum phase shift transition between symbols is only $\frac{1}{2}\pi$, which limits the used bandwidth if pulse shaping is applied. TETRA uses a root raised cosine filter to reduce the bandwidth [23].

The frame structure is shown in Figure 3. One time slot consists of 255 symbols or 510 bits. The voice data is divided into speech frames of each 30 milliseconds. Two of these speech frames fit into a single transmission burst (or time slot). Four time slots form a frame and eighteen of these frames form a multiframe. A multiframe is 1.02 seconds long. Seventeen pairs of speech frames are fitted into 17 frames. This means that every multiframe has one frame left (30 ms $\cdot 17 \cdot 2 = 1.02$ s equals the time of one multiframe). Frame 18 is the remaining frame and is used for control signals. The uplink and download of the data is on different time slots. Therefore, full duplex communication is possible. One frame exists between the uplink and download slots, such that the system has time to switch from transmit mode to receive mode.

A physical channel is defined for a specific carrier frequency and TDMA slot number. There are two kinds of physical channels: control physical channels and traffic physical channels. Onto these physical channels several logical channels are multiplexed after they are fit into bursts. The routing of the logical channels to the physical channels is handled by the lower MAC layer of the data link layer.

Signals that are transferred over the control physical channels include TDMA information. To ensure that the mobile is aligned with the modulated symbols and the frames of the base station a synchronisation has to be performed. Furthermore, it is necessary that the receiver is aligned with the transmitted symbols. A training sequence is a known sequence of symbols which the receiver attempts to detect. The receiver makes use of the training sequence to achieve synchronisation by cross-correlating the training sequences [20]. A low cross correlation is desired between a random data sequence and the training sequence, so that no false triggering will occur.

Fig. 1: Constellation diagram $\pi/4$-DQPSK

Fig. 2: Constellation diagram $\pi/4$-DQPSK shifted by 45°

Fig. 3: TETRA frame structure taken from [2]
TABLE I: Main physical layer parameters for TETRA [21]

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carrier spacing</td>
<td>25 kHz</td>
</tr>
<tr>
<td>Modulation</td>
<td>π/4-DQPSK</td>
</tr>
<tr>
<td>Carrier data rate</td>
<td>36 kb/s</td>
</tr>
<tr>
<td>Voice coder rate</td>
<td>ACELP (4.56 kb/s net, 7.2 kb/s gross)</td>
</tr>
<tr>
<td>Access method</td>
<td>TDMA with 4 time slots/cARRIER</td>
</tr>
<tr>
<td>User data rate</td>
<td>7.2 kb/s per time slot</td>
</tr>
<tr>
<td>Maximum data rate</td>
<td>28.8 kb/s</td>
</tr>
<tr>
<td>Protected data rate</td>
<td>Up to 19.2 kb/s</td>
</tr>
</tbody>
</table>

More information about training sequences can be found in [21]. TETRA uses several training sequences. It can be roughly divided in training sequences used for synchronisation with the modulation symbols and training sequences used for synchronisation with the TDMA frames [20]. The first training sequence is a short sequence of 22 bits and is transmitted in every burst. The second one is an extended training sequence, which is transmitted in every multiframe on the control physical channel. It is also transmitted on a traffic physical channel, but shares the burst with other signalling blocks. The exact algorithm of the synchronisation in the receiver is not specified and depends on the implementation.

Delay is an important aspect in the physical layer especially if dealing with speech data [21]. TDMA allocates time slots to the user, which the user can use to transmit or receive data. An inherent problem of TDMA is delay: data is not transmitted continuously. The system has to wait for its specified time slot to transmit data. Furthermore, the system also needs to buffer long data packets which do not fit in one slot and the continuous speech data has to be fitted into 17 of the 18 frames. So the speech data has to be sent faster than it is produced by the speech coder in order to transmit in 17 frames. This means that all the speech data has been sent after the 17th frame and thus the buffer for one multiframe is empty after the 17th frame. Of course, more time slots can be allocated to the user increasing the throughput of one user, but decreasing the capacity of the system.

A scrambling sequence is applied to prevent regular patterns in the transmitted data [21]. The scrambling prevents that the data stream causes unwanted frequency components and synchronisation problems. The power density will be equally spread in-band. Since TETRA uses a differential modulation scheme, this does not apply in this case. However, continuous 0s and 1s will cause tones in the output. Between base stations each has a different scrambling sequence. So that a mobile in a different cell does not cause false messages. Scrambling is not used to prevent eavesdropping. If you listen to the initial control messages and discover the shift register sequence, then you have sufficient information to decode the scrambling. Protection against eavesdropping is done on the air interface or at the application layer with cryptographic protocols. Other functions on the physical layer such as power control and coverage techniques will not be discussed, because they are not relevant for IEMI purposes.

The main function of the data link layer is to provide an error free communication between the transmitter and the receiver [2]. The physical layer provides the data link layer with a raw bit pipe for information. It adds error detection and error control techniques. It also schedules transmission of data provided by the network layer.

The data link layer is divided into three sub layers. The lower medium access control (MAC), the upper medium access control, and the logical link control (LLC) [21]. The lower MAC provides the physical layer with the raw bits and ensures that the right data is sent in the right TDMA slot. For example, frame 18 is the control frame and thus used for signalling purposes and not for speech data. Other functions of this layer includes interleaving and slot stealing. An overview of the interfaces in the error control structure is shown in Figure 4. Depending on the logical channel it passes or skips these error control schemes. Several of these logical channels are shown in Figure 5. The Access Assignment Channel (AACH) is coded with a shortened Reed Muller code, but is not interleaved nor convolutional coded.

The upper MAC layer performs access control, signalling and traffic functions, and air interface encryption. The main function of the logical link control is to provide error free data to the network layer. It attains this by organising retransmissions, segmentations, and reassembly. Finally, the logical link control coordinates the logical links.

The network layer uses the data link layer to provide bearer services which are basic communication services that concerns how data is transported from point to point [2]. The bearer services of the network layer makes it possible for higher OSI layers to implement more advanced functions and services without having to worry about the underlying radio technology. The bearer services that a TETRA system provides are individual call, group call, acknowledged group call and broadcast call for circuit mode, and packet connection oriented mode and packet connectionless mode [21]. The network layer is also responsible for the mobility management. This service distinguishes a mobile network from a fixed network. Since mobiles can move freely and can therefore switch between cells it is necessary to keep track of all users. This is achieved by registering and de-registering mobiles in a mobile database. The location area is saved as well. The mobility management also informs mobile stations about incoming calls (paging). Finally, the network layer provides supplementary services. These services include among others services such as call identification, call forwarding, call offering, call completion, call restriction, and call intrusion services.

B. TETRA sensitivity to IEMI

In the previous subsection an introduction to the TETRA protocol is given. With this information it is possible to

TABLE II: Phase transitions for π/4-DQPSK

<table>
<thead>
<tr>
<th>Dibit</th>
<th>Phase transition</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>π/4</td>
</tr>
<tr>
<td>01</td>
<td>3π/4</td>
</tr>
<tr>
<td>11</td>
<td>−3π/4</td>
</tr>
<tr>
<td>10</td>
<td>−π/4</td>
</tr>
</tbody>
</table>
expose vulnerabilities in the protocol to determine if TETRA is resilient against intelligent IEML. Several jamming strategies such as spoofing, Distributed Denial of Service (DDoS), and disrupting the synchronisation procedures are now analysed. The Access Assignment Channel proves to be critical for correct functioning of the slotted ALOHA procedure.

In TETRA the layers above the MAC layer are encrypted. It is therefore difficult to obtain the original messages. Furthermore it is difficult to spoof the communication system since all TETRA devices have TETRA Equipment Identification (TEI) numbers, which uniquely define each device [21]. Jamming of the sent voice data is possible, but it requires more energy since it is required to interfere the voice data continuously. Furthermore, since power is constantly transmitted, it is easier to detect that the system is being jammed.

However, the system is vulnerable to interruptions to the right control messages. The advantage of this technique compared to the naive jammers is that the jammer is more likely to stay covert, since it does not have to send signals continuously as in the case of the constant and deceptive jammer. It hits the critical control packets instead of sending random bits and corrupting random packets. Furthermore, the jammer is more energy efficient, since it is not constantly sending interference signals [17]. TETRA has already been tested with Additive White Gaussian Noise on the channel with the simulation package TETRASIM [24], but interference signals acting on specific control data packets have not been reported to the knowledge of the author.

DDoS attacks can be created against TETRA, but it requires more power to generate the many synchronisation messages with the base station compared to generating an interference signal at the right time. Also most importantly, the system can be more easily detected since it receives many messages with an invalid TEI number.

However, this does not mean that TETRA is immune to all intelligent jamming. TETRA is a wireless system and since it uses TDMA the mobile and the base station have to synchronise each time a communication session is started. This synchronisation is not protected. The base station sends the unencrypted synchronisation block periodically. The training sequences are known so that the mobiles can lock onto it [20]. If the synchronisation is disturbed, the mobile cannot synchronise with the base station and the communication link cannot be set up. This way of jamming requires listening to the channel and determining when the synchronisation block is sent and subsequently interfere with this signal. Jamming this signal will only work if the mobile did not have established a connection with the network already. However, since the mobile sets this connection at start up of the device, at a non critical moment it is not very effective.

Another better possibility to paralyse the TETRA system is to interfere the random access protocol. This protocol is based on slotted ALOHA procedures and is extended with an access framing structure. The random access protocol with slotted ALOHA is used when a mobile wants to transmit an unsolicited message to the base station. The mobile station does not have a reserved channel and has to use this protocol. The base station sends so called “Access Codes”. There is a maximum of four possible access codes. The base station sends these codes to mark opportunities for the mobile stations to start a transmission. Mobile stations will only try to send traffic in these designated frames. This way the control of collisions of access requests from different mobile stations is taken care off. It is also possible to provide different kind of grades of service. The access codes are sent on the Access Assignment CChannel (AACH). The AACH is sent in the Broadcast Block of every downlink frame. The mobile will wait for the correct access code before transmitting. In the ETSI TETRA protocol standard the following is stated: “If the AACH is not decodeable then both the corresponding uplink subslots shall be regarded as reserved” [20]. Thus it regards the uplink slot as not available for random access or common linearisation. So according to the protocol it is possible that the mobile will wait indefinitely if it cannot decode the AACH message. However, if the base station contacts the mobile then it still can setup a link since it will reserve slots for the mobile to send its data. Nevertheless, the impossibility for the mobile station to setup a link can be troublesome for
emergency services, e.g., it is hard to call for assistance or to brief the situation of the emergency. The AACH message is generated in the MAC layer and it consists of 14 bits which are sent in the broadcast block of each burst. Before these 14 bits are sent to the physical layer for transmission it is first encoded with a shortened Reed Muller code into 30 bits and then the resulting 30 bit long stream is scrambled. This scrambled 30 bit long code is then put in the broadcast block of the burst.

C. Modulation scheme

It is now known which control messages of the protocol should be interfered with to disrupt the system. Now these messages have to be interfered with a signal that creates bit errors in the messages, while being able to stay covert. What kind of signal is effective at creating errors at the receiver is now discussed. The message signals are interfered with in the ether, since the nature of the medium is shared and thus easy to access for jammers. Signals distributed over the spectrum are more likely to stay covert compared to continuous wave signals.

To achieve errors in the modulation scheme the points in the constellation diagram have to be shifted over the decision boundaries, or with other words the error vector magnitude (EVM) has to be increased. The EVM is a measure for how much the constellation point is shifted away from the correct position in the constellation diagram. There are two diagrams with different decision boundaries for the π/4-DQPSK scheme because of the π/4 shift after every symbol as shown in Figure 2. It is too complex to determine in which diagram the receiver is receiving the bits and therefore an interference has to be created which creates a large enough EVM to shift the points for both diagrams over the decision boundaries. In the first scheme, the probability that a constellation point is pushed over a boundary is 0.5 and in the second scheme the probability is 0.75 as seen in Figure 6, if the amplitude of the jamming signals is larger than the modulated signal. In this analysis the QPSK interference signal is synchronised with the π/4-DQPSK signal to be able to push the points over the decision boundaries as shown in Figure 6. Also the QPSK signal has to be exactly in the bandwidth of the π/4-DQPSK signal. Furthermore, it is assumed that the signals are exactly synchronised to achieve the superposition. In the practical situation this is never the case. The phase noise and the frequency difference between the interference and the modulation signal will rotate the QPSK signal around the π/4-DQPSK points. In addition, the sampling points to determine the symbols for the π/4-DQPSK and the QPSK are not in synchronisation. Therefore the QPSK signal will not be sampled on the four points, but also somewhere along the signal trajectory between the four points.

It is also possible to interfere with a continuous wave. Consider the incoherent demodulator shown in Figure 7, where \( x_n(t) \) is the data signal, \( m(t) \) is the interference continuous wave signal.

\[
x_n(t) + m(t) = a \cos(\omega t + \phi_n) + b \cos(\omega t + \Delta \omega t + \phi_m)
\] (1)

Where \( a \) is the amplitude of the modulated signal, \( \omega \) the angular frequency, \( t \) the time, \( \phi_n \) the modulated phase, \( \phi_m \) the phase of the interference, and \( \Delta \omega \) the difference angular frequency between the modulated signal and the interference. This signal is received by the demodulator and most demodulators demodulate the transmitted signal by multiplying the received signal with an oscillator and either integrate or filter the signal as can be seen in Figure 7. The resulting signals are the points on the constellation diagram: \( X_n \) and \( Y_n \), which are the in-phase and quadrature components, respectively. These signals are then further processed depending on the demodulator. The signals \( X_n \) and \( Y_n \) in Figure 7 are obtained by multiplying the data signal \( x_n(t) \) and the interference signal \( m(t) \) with the local oscillator and subsequently integrate the resulting signal.

\[
X_n = \int_0^T (a \cos(\omega t + \phi_n) + b \cos(\omega t + \Delta \omega t + \phi_m)) \cdot \cos(\omega t + \phi_d) dt = \frac{aT}{2} \sin(\phi_n + \phi_d) + \frac{bT}{2} \sin(\Delta \omega t + \phi_m + \phi_d)
\]

\[
Y_n = \int_0^T (a \cos(\omega t + \phi_n) + b \cos(\omega t + \Delta \omega t + \phi_m)) \cdot \sin(\omega t + \phi_d) dt = \frac{aT}{2} \cos(\phi_n + \phi_d) + \frac{bT}{2} \cos(\Delta \omega t + \phi_m + \phi_d)
\] (2)

Where \( T \) is the integration time, and \( \phi_d \) is the phase of the local oscillator. From the calculation it can be seen that the constellation diagram rotates with the difference frequency between the continuous wave and the carrier wave of the data signal. If the interference is on the centre frequency and is also phase synchronised, then only a constant offset in the constellation diagram is added.

The probability that a point is pushed over a boundary, or symbol error probability (SEP), depends on the amplitude of the wave. Figure 8 shows there are three domains depending on the amplitude \( r \) caused by the continuous wave interference. The fraction of the circle that crosses over the dashed threshold lines is now determined. There are three domains: domain \( a \) is for \( r < x \), domain \( b \) for \( x < r < \sqrt{2}x \), and domain \( c \) for \( \sqrt{2}x < r \), where \( x \) is the distance from the constellation point to the threshold. The SEP caused by the continuous wave is 0 in situation \( a \) of Figure 8. The SEP for domain \( b \) can be obtained by using geometry:

\[
\theta = \arccos\left(\frac{x}{r}\right)
\] (3)

\[
p_e = \frac{4 \cdot \arccos\left(\frac{x}{r}\right)}{2\pi}
\] (4)

Where \( \theta \) is the angle as defined in Figure 8 and \( p_e \) is the SEP. And finally, the SEP is for domain \( c \):

\[
\theta = \arccos\left(\frac{x}{r}\right)
\] (5)

\[
p_e = \frac{2 \cdot \arccos\left(\frac{x}{r}\right) + 1/2\pi}{2\pi}
\] (6)

For the limit of \( r \) to infinity the probability will become 0.75. Of course this is theoretical possible, but once 0.5 is reached, it is the same as a random sequence. Note that in
this analysis it is not taken into account how the receiver will respond after receiving an erroneous symbol. It is assumed that the constellation diagrams are superposed and the demodulator decides based on the superposition.

A standard Simulink model has been adapted to determine the effect of an interference on the channel, see Figure 9. If a continuous wave is added to the channel to interfere with the modulated signal it is expected that the interference is superimposed on the original constellation diagram. A QPSK modulated interference is also simulated as interference.

Fig. 6: Constellation diagram with QPSK

Fig. 7: Incoherent demodulator for $\pi/4$-DQPSK taken from [25]

Fig. 8: Constellation diagram with an interference continuous wave

Fig. 9: $\pi/4$-DQPSK Simulink model

Fig. 10: Constellation diagram of $\pi/4$-DQPSK with continuous wave interference

Fig. 11: Constellation diagram of $\pi/4$-DQPSK with a synchronised QPSK interference

Fig. 12: Constellation diagram of $\pi/4$-DQPSK with large QPSK interference. The green points are the $\pi/4$-DQPSK signals that are interfered with. The resulting constellation points are the blue points.
Figures 10, 11, and 12 show that the superposition is indeed the case both for small amplitudes of interference and large amplitudes. Of course, the results in the simulations with the larger amplitudes are not realistic, since in a realistic situation the receiver gets out of synchronisation before the results in the simulations are obtained. The graph in Figures 13 and 14 shows the spectra. It can be clearly seen that the continuous wave creates a spike in the spectrum, while the power of the QPSK interference is divided over the whole spectrum.

D. Jammer

A jammer is now proposed that combines the knowledge of the vulnerabilities and a way to interfere with bits on the physical layer, that is acquired in the previous subsections. It is analysed whether the jammer is able to stay covert against several jamming detection techniques.

The most commonly used criteria to determine jamming efficiency are: energy efficiency, probability of detection, level of denial of service, and resistance to physical layer anti-jamming techniques [8]. All of these criteria are important, but depending on the situation one of these criteria will be the main aim. In addition to these criteria, intelligent jammers have the following goals as stated in [8], [26]: maximise jamming gain, target jamming, and reduced probability of detection. Intelligent jammers try to exploit upper layer protocols to achieve these goals [8].

In the previous sections it is shown that the TETRA communication system can be disrupted to a level that the mobile stations cannot start calls. This is achieved by interfering with the AACH messages sent by the base station. The jamming gain is improved considerably, since in every frame, which contains 510 bits, only 30 bits have to be disrupted to make sure the mobile stations cannot start calls. The probability of detection of the jammer can be reduced by using a QPSK modulated signal as the interference signal. As shown in the previous section, the signal is divided over the spectrum, which makes it hard to detect the jammer. Furthermore, it is not straightforward to discriminate jamming from the legitimate traffic scenarios using only the signal strength [17]. This discrimination between legitimate and adversarial traffic is also the main challenge for detection of jammers. The reason for poor connectivity can be caused by either legitimate causes or adversarial causes [17]. This is another point the jammer takes advantage of by interfering with the AACH messages. If the AACH messages are attacked it appears from the mobile station point of view as if the network is congested, since the devices cannot make new connections, but running conversations are not affected.

Other data besides the signal strength are analysed such as the packet delivery ratio (PDR). Even if a network is congested the PDR always maintains a certain PDR value, while an effective jammer decreases the PDR to a value close to zero [17]. However, this method cannot be applied to detect the jamming attack described in this thesis. Conversations cannot be started by the mobile stations by attacking the AACH. There is no steep drop in PDR, since an ongoing conversation is not terminated.

More advanced jamming detection strategies include combining the PDR and the signal strength [17]. The idea behind combining the data is that a low PDR should be caused by a low signal strength if it is caused by legitimate causes. For example, this situation can occur if the mobile station is too far away from the base station. However, if an effective jammer is active the signal strength is high, but the PDR low. This information is then used to detect jammers. The jammer circumvent this detection, since there is no data for the PDR, because no new conversation can be started and ongoing conversations are not interrupted.

---

![Fig. 13: Spectrum of \(\pi/4\)-DQPSK (black) and continuous wave interference (red)](image1.png)

![Fig. 14: Spectrum of \(\pi/4\)-DQPSK (black) and QPSK interference (red)](image2.png)
TETRA base stations perform jamming detection techniques. They look at the synchronisation of the bits. If these are out of synchronisation they can determine that they are being jammed. However, this jammer is interfering with the mobile station, if the base station is uploading. Therefore, the jammer will not be detected by the base station’s jamming detection techniques.

So a jammer that interferes with the AACH and uses a QPSK signal is effective at disrupting the TETRA communication system, while being able to stay covert. It is now known which part of the TETRA protocol should be interfered with to ensure that mobile stations cannot start new calls and to stay covert. To disrupt the bits a certain jamming-to-signal ratio (JSR) is required. This ratio is given by the following equation [27]:

\[
\frac{J}{R} = \frac{P_j G_{jr} G_{rt} R_{jr}^2 L_r B_r}{P_l G_{lr} G_{rt} R_{rt}^2 L_j B_j}
\]  

(7)

Where \(P_x\) is the power of the jammer or intended transmitter; \(G_{xx}\) the gain between the jammer and receiver or transmitter and receiver; \(R_{xx}\) the distance between jammer and receiver or transmitter and receiver; \(L_x\) the loss in the receiver or transmitter; and \(B_x\) the bandwidth of the receiver or jammer. Increasing this ratio will increase the effectiveness of disrupting bits. However, it will also increase the possibility of detection. The terminals of TETRA are specified to operate with a signal to interference ratio of 19 dB. The dynamic receiver sensitivity of the base station and mobile station is -106 dBm and -103 dBm, respectively [21]. Therefore the jammer should create a signal that is no more than 19 dB lower than the modulated signal, when the jamming signals arrives at the mobile station.

The jammer’s block diagram is shown in Figure 15. The first part is the demodulator. The demodulator has to correctly down convert the signal received from the antenna and correlate the training sequence to synchronise with the base station. If the jammer is synchronised a signal is sent to the second part, the counter. The counter has to count till the base station is about to send the AACH message in the broadcast block. Then the counter signals the transmitter to generate the interference signal and the counter is reset.

### III. Measurement Setup

In Section II, it is shown that an interference signal that is distributed over the spectrum is more likely to stay covert than a continuous wave. In this section a measurement setup is described, where a vector signal analyser (VSA) was connected with two vector signal generators (VSG) via a power combiner. The goal of the measurements was to verify the superposition of the interference with the modulated signal and to determine whether the interferences could stay covert or were easily detectable.

The measurement setup shown in Figure 16 was used to measure the superposition and spectra. The VSA was an Agilent PXA Signal Analyzer N9030A, the modulating vector signal generator (mVSG) to create the modulation signal on a frequency of 390 MHz was an Agilent E4438C ESG VSG, and the interfering vector signal generator (iVSG) to create the interference was an Agilent E8267D PSG VSG. The used power combiner was an ZFRSC-123-S+ from Mini-Circuits. The VSA measured the constellation diagram and the spectrum. The following settings were set for the mVSG: centre frequency at 390 MHz, power at -40 dBm, \(\pi/4\)-DQPSK modulation, and a symbol rate of 18 kbps. The iVSG used two different interference signals: a continuous wave and a QPSK modulation scheme. The power of the interference was set at -50 dBm at the centre frequency and at 1000 Hz above the centre frequency of the modulated signal. The iVSG and mVSG were synchronised and unsynchronised by connecting and not connecting the 10 MHz reference signal, respectively. The iVSG sent random bits with QPSK modulation.

### IV. Measurements

In this section the measurements are shown described in Section III. The constellation diagrams and spectra are shown for synchronisations and different frequencies. The QPSK signal created a smaller EVM, but was less noticeable in the spectrum than a continuous wave. The VSA lost synchronisa-
tion, when the constellation points started to overlap with the neighbouring constellation points.

The constellation diagrams are shown in Figures 17 and 18 and the spectra are shown in Figures 19 and 20. When the continuous wave had the same centre frequency and was synchronised via the 10 MHz as the $\pi/4$-DQPSK, the interference did not affect the constellation diagram. The continuous wave adds a constant shift in the diagram, but the VSA compensates for this constant shift. Therefore, this shift is not visible in this plot. The QPSK signal, however, does create an error vector magnitude and as expected the QPSK signal is superimposed on the $\pi/4$-DQPSK signal. Measurements were performed with larger amplitudes, but then the VSA could not lock on the signals and the $\pi/4$-DQPSK constellation could not be reconstructed. The error vector magnitude readings also increased and varied greatly.

When the continuous wave was not synchronised and set at 1000 Hz above the centre frequency, the constellation rotated, which is in accordance with Equation 2. The asynchrony and setting the frequency 1000 Hz above the centre frequency of the $\pi/4$-DQPSK resulted in a cloud of points around the constellation points when a QPSK interference was added. This is caused since the signal is on a trajectory to the QPSK points, but is not sampled at times when the QPSK points are reached. The phase noise also caused the constellation points to rotate. The continuous wave created a larger error vector magnitude than the QPSK signal.

In Figure 19, two clear peaks can be seen at the centre frequency and 1000 Hz above the centre frequency, which are caused by the continuous wave interference. The QPSK interference does not cause a noticeable different spectrum as shown in Figure 20. The continuous wave at 1000 Hz above the centre frequency caused a larger error vector magnitude than the QPSK signal, while also causing a peak in the received spectrum. The QPSK signal, however, did not created a noticeable difference in the received spectrum.

V. DISCUSSION

The purpose of this thesis is to investigate the resilience of TETRA against intelligent intentional electromagnetic interference. Specifically, a closer look is taken at the TETRA protocol and the modulation scheme.

The protocol is studied in Section II-A. From this analysis it is concluded that it is not very effective to corrupt the speech data. The speech data passes error control schemes and the data is split into bits of different priorities. The most important bits receive a lot of error protection and therefore interfering with these data bits requires corrupting the bit stream during the conversation. Since the interference is almost continuously active, it can be detected relatively easily by measuring the received signal strength [17]. If the interference is detected, the system can take counter measures to reduce the impact of the jammer.

The analysis of the TETRA protocol shows it is also protected against spoofing, since each TETRA equipment has to have a registered equipment number. Without a registered number it is not possible to start a conversation. All registered numbers are stored in databases and once a device is obsolete or is lost, the number can be stripped of the permissions to make calls and send data. Furthermore, listening to messages on the channel is hard, since the data is encrypted. Distributed denial of service attacks are not effective as well, since it requires a lot of resources and the base station can detect that a lot of unauthorised requests are made for conversations.

In Section II-B it is shown that if the AACH cannot be decoded, the TETRA protocol states that it will then wait indefinitely. The mobile station does not know when it is allowed to start a transmission. If the mobile station would start a transmission at a random moment, then it could interfere with another legitimate conversation. This finding means that if the AACH is disrupted the communication system can be affected quite badly, because the mobile stations cannot

![Fig. 17: Constellation diagram without IEMI (red); and with continuous wave IEMI on the centre frequency (blue) and 1000 Hz above the centre frequency (green).](image1)

![Fig. 18: Constellation diagram without IEMI (red); and with QPSK IEMI on the centre frequency (blue) and 1000 Hz above the centre frequency (green).](image2)
start a conversation. The interference is hard to detect and therefore stays covert. Counter measures against jamming is difficult, since it is unable to decide whether the drop in communication is caused by legitimate reasons, e.g. reduced signal, or by adversaries. It is hard to detect, because only at specific moments for short periods the interference corrupts signals. The error detection occurs at the base station while the jammer transmits its interference when the base station is transmitting.

Several conclusions can be drawn from the results in Section IV. Figure 17 indicates that it is not very useful to interfere with a continuous wave at the centre frequency. If the continuous wave is at the centre frequency and in exact phase as the intended modulated signal, then the interference causes only an offset in the constellation diagram. This offset can be easily compensated for. However, Figure 18 shows that the QPSK modulated interference does create an EVM. The constellation diagram is the superposition of the $\pi/4$-DQPSK signal and QPSK signal.

Exact synchronisation with the TETRA signal is in practice hard to achieve and therefore the asynchronous results are more realistic. These show that the continuous wave creates a larger EVM compared to the QPSK signal. The QPSK signal causes a cloud of points around the $\pi/4$-DQPSK constellation points. This is because the signal is not sampled at the exact time when the QPSK reaches its own constellation points and this causes the point to be sampled along its trajectory. Furthermore, the asynchrony causes a phase shift.

Although the QPSK interference creates a smaller EVM, the spectra in Figures 19 and 20 demonstrate that the QPSK interference is not noticeable in the spectrum, while the continuous wave can be clearly seen. From this it is concluded that the continuous wave signal is more easily detectable, if interfering with a bit stream modulated with $\pi/4$-DQPSK. This is in accordance with the study performed by Mleczko et al [28], where they also show that a signal occupying a significant amount of the bandwidth requires a lower signal level. The experiments also showed that the VSA lost synchronisation if the power difference between the interference and $\pi/4$-DQPSK signal is smaller than 10 dBm. This was the case for both the continuous wave and the QPSK modulated signal. From an intelligent jammer perspective it is important to stay covert, since no detection means that no counter measures will be taken against the jammer. Therefore, this research shows it is best to use a QPSK signal to interfere with the $\pi/4$-DQPSK signal even if the signals are not synchronised.

The research shows that the TETRA protocol has already several procedures implemented to protect itself against adversaries. Basic attacks such as a continuous jammer can be effective at corrupting bits, but can be detected. Counter measures can then be taken. Spoofing the system is also hard, because all equipments have registered identification numbers. Although a distributed denial of service attack by flooding the base station with requests is possible, it is easily detectable and requires a lot of power and resources. However, the research demonstrates that if a jammer is able to synchronise with the base station and corrupts the AACH data, then the mobile stations are not able to start conversations. This jammer is more difficult to detect since it is only transmitting for a short time. Adversaries could exploit this theoretical finding by implementing a jammer that focusses on disrupting the AACH data.

An adversary can interfere with the modulation scheme the best using a continuous wave that is not at the exact centre frequency and is not phase synchronised. This signal creates the largest EVM. However, if looking from the point of view of an adversary it is better to use a QPSK signal. This signal is divided over the spectrum and is harder to detect as is in agreement with [28].

There are some limitations to this research. The vulnerability found in this study still has to be verified with real TETRA equipment. The bit error rates also have not been
properly measured. The simulations are synchronised and plots of the superposition of the π/4-DQPSK signal and the QPSK signal are obtained. However, in the real world the signals are not synchronised. In the experiments it was shown that the VSA could not lock onto the constellation points, because the constellation points started to overlap. These experiments can only show what the effect is of the interference on the EVM. There is a relation between the EVM and the bit error rate, but it cannot be said with certainty that one value for the EVM corresponds to another value for the bit error rate.

VI. Conclusion

TETRA, the voice communication component of the emergency services communication system C2000, can be disrupted by an intelligent jammer. The slotted ALOHA protocol can be interfered with by corrupting each AACH block, since the TETRA protocol states that the mobile station will wait indefinitely before transmitting until the AACH can be decoded. The study also showed that an IEMI 10 dBm lower than the intended signal was able to create a large EVM. The continuous wave interference caused a larger EVM than the QPSK modulated interference. However, a QPSK modulated interference stays covert, while a continuous wave with the same power causes a noticeable peak in the received spectrum compared to the situation without any interference.

For future work it is recommended to perform bit error rate measurements to determine if the QPSK interference is still able to stay covert while achieving a large bit error rate. Different modulation schemes occupying a significant part of the wanted signal should be investigated that create a large bit error rate while staying covert. A TETRA setup including a base station and mobile station should be set up. The rough outline of the jammer described in this thesis should be implemented and connected to this setup to verify whether the mobile station cannot setup a conversation once the jammer is active. The results in this thesis already raises more issues. TETRA is not completely protected against intelligent jamming attacks and it is now required to address how to protect the system against these kinds of attacks. This study revealed a possible vulnerability in the protocol that adversaries could exploit and therefore further research is required to determine if there are even more possible weaknesses.

ACKNOWLEDGMENT

The author would like to thank F.B.J. Leferink, M.J. Bentum, and G.J. Heijenk for participating in the exam committee; G.S. van de Beek for providing day to day help and support during the project; H. de Vries and E.V. Bos for providing extensive help in the lab; and the students in the ICD/SC/TE student room and the people of the Telecommunication Engineering group of the University of Twente for providing a pleasant work environment.

REFERENCES