# Vulnerability of Terrestrial-Trunked Radio to Intelligent Intentional Electromagnetic Interference

Ray R. Tanuhardja, Stefan van de Beek, *Student Member, IEEE*, Mark J. Bentum, *Senior Member, IEEE*, and Frank B. J. Leferink, *Senior Member, IEEE*

***Abstract*—The terrestrial-trunked radio (TETRA) specification is produced by the European Telecommunication Standards Institute for private mobile radio systems. We investigated the resilience of TETRA against intelligent intentional electromagnetic interference (IEMI) with low amplitude. Low power signals interfering with the higher layers of the system 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 quadrature phase shift keying (QPSK) is interfered with a continuous wave and a QPSK signal. The results show that a continuous wave created the largest error vector magnitude, 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 is more effective as an intelligent interference signal compared to a continuous wave. In this paper, it is shown that it is possible to create an IEMI that combines the vulnerability in the TETRA protocol with the QPSK signal to disrupt the service to the communication system, while staying covert.**

***Index Terms*—Communication system protocol, intelligent jammer, intentional electromagnetic interference, terrestrial-trunked radio.**

## I. Introduction

TETRA was developed by ETSI to replace the previous analogue PMR systems [1]. The advantages of the digital TETRA system are the utilisation of data communication, the robustness, and the encryption of traffic [1]. Another important advantage is the relatively low frequency it operates on, giving the transmitters a long range [2]. Thus, such systems require less base stations, cutting the infrastructure costs.

With the increase of wireless communication systems and electromagnetic interference, the ether is becoming more and more crowded. TETRA was developed for public safety organisations and therefore it is crucial that the system stays online even with some interference. However, it is also interesting to consider to what extent the system is able to resist intentional attacks. By recognising the possible vulnerabilities, it is possible to take adequate countermeasures and increase the security of the system.

Wireless communication systems are especially sensitive to attacks from adversaries, since the nature of the medium is shared and easy to access [3]. There are several examples of jammers that are commercially available that interfere with other wireless communication systems [4]–[6]. There are several low power IEMI jammers possible: constant jammers, deceptive jammers, random jammers, reactive jammers, and intelligent jammers [7]. More information about the first four jammers can be found in [3], [7], [8]. This research focusses on intelligent low power jammers, which exploit weaknesses in higher layers of the open systems interconnection (OSI) model to impair the correct functioning of the communication system with very low energy jamming and deny users access to the service. These jammers require extensive information of the victim's protocols and are more complex to implement.

Smart jamming attacks on wireless systems have already been investigated. Jamming attacks focusing on the synchronization procedures of the GSM network can successfully deny mobile terminals [9]. There are even more smart jamming attacks focusing on the IEEE 802.11 protocol. Corrupting the clear to send messages and acknowledgment 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 [3]. Although, TETRA has been tested with additive white Gaussian noise, smart jamming attacks focusing specifically on TETRA have not yet been investigated. Therefore, it is still unknown whether adversaries are able to compromise the system.

This study focuses on low power IEMI attacks via the front door to interfere with the modulation scheme and protocol of TETRA. The first advantage of such a technique 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 [10] and by using low power, systems can stay small.

In Section II, TETRA's sensitivity to IEMI is investigated by the analysis of the TETRA protocol. How to interfere with the symbols on the physical layer is examined in Section III. In Section IV, an intelligent jammer is evaluated. In Section V, the results of measurements of the superposition of the digital modulation scheme are shown. The study is concluded in Section VI.

Manuscript received June 12, 2014; revised September 22, 2014; accepted October 24, 2014. Date of publication January 30, 2015; date of current version June 11, 2015.

R. R. Tanuhardja and S. van de Beek are with the Telecommunication Engineering Group, University of Twente, 7522 NB Enschede, The Netherlands (e-mail: r.r.tanuhardja@alumnus.utwente.nl; g.s.vandebeek@utwente.nl).

M. J. Bentum is with the Telecommunication Engineering Group, University of Twente, 7522 NB Enschede, The Netherlands, and also with the Netherlands Institute for Radio Astronomy ASTRON, 7991 PD Dwingeloo, The Netherlands (e-mail: m.j.bentum@utwente.nl).

F. B. J. Leferink is with the Telecommunication Engineering Group, University of Twente, 7522 NB Enschede, The Netherlands, and also with Thales Netherlands, 7550 GD Hengelo, The Netherlands (e-mail: frank.leferink@utwente.nl).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TEMC.2014.2385893

## II. Vulnerabilities

Intelligent jammers are devices which exploit higher layers of the OSI model to interfere with a communication system. Therefore, a lot of prior knowledge of the system is required. Readers not familiar with the TETRA protocols can find more information in [11]–[13]. The vulnerabilities of these protocols are now exposed.

### *A. Distributed Denial of Service (DDoS) Attacks*

In TETRA, the upper medium access control layer provides air interface encryption [12]. 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 [11]. Without a registered TEI 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 its permissions to make calls and send data. A commonly used attack is a DDoS attack [14]. There are several ways to perform such an attack, but the main goal is always to deny users from service. For example, a DDoS attack can create a large number of communication requests that saturates the target device, so that it cannot respond to legitimate traffic. These attacks can also be generated against TETRA and do not necessarily require valid TEI numbers. However, it requires more power to generate the many synchronization 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.

### *B. Interfering With the Voice Data*

Jamming of the sent voice data is the most easy and crude way to deny users from service. However, it requires a lot of energy since it is required to interfere with the voice data continuously. 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 complete bit stream during the conversation. Since the jammer needs to transmit interference signals continuously, it can be detected relatively easily by measuring the received signal strength [8]. If the interference is detected, the system can take countermeasures to reduce the impact of the jammer.

### *C. Interfering With the TDMA Synchronization*

There is a more intelligent way to interfere with the system than just simply occupying the channel by transmitting continuously. The system is vulnerable to interruptions of the correct 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 [8]. TETRA has already been tested with additive white Gaussian noise on the channel with the simulation package TETRASIM [2], but interference signals acting on specific control data packets have not been reported to the knowledge of the authors.

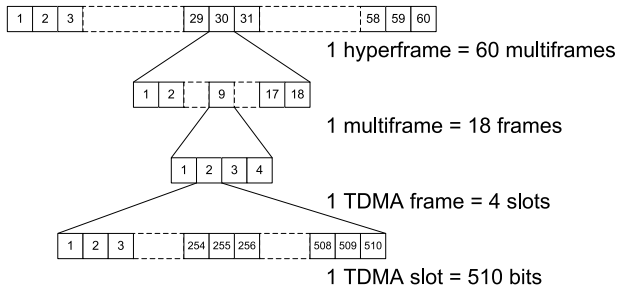



Fig. 1. TETRA frame structure. Each TDMA slot assigned for downlink channels contains a broadcast block[12].

TETRA uses TDMA and therefore the mobile and the base station have to synchronize each time a communication session is started. This synchronization is not protected. The base station sends the unencrypted synchronization block periodically. The training sequences are known so that the mobiles can lock onto it [12]. If the synchronization is disturbed, the mobile cannot synchronize 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 synchronization block is sent and subsequently interfere with this signal. Jamming this signal will only work if the mobile has not established a connection with the network already. However, since the mobile sets this connection at start, a noncritical moment, it is not very effective.

### *D. Interfering With the Access Assignment Channel (AACH)*

Another better possibility to paralyse the TETRA system is to interfere with the random access protocol. This protocol is based on slotted ALOHA procedures [15]. The slotted ALOHA procedures are 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 time frames. This way the control of collisions between access requests from different mobile stations is taken care off. It is also possible to provide different kinds of grades of service. For convenience, the TETRA frame structure is shown in Fig. 1. One TDMA slot is 510 b long. Each TDMA slot assigned for data transmission from base station to mobile station, i.e., a downlink, contains a broadcast block. The access codes are sent on the AACH. The AACH is sent in the broadcast block of every downlink slot and it consists of 14 b. Before these 14 b are sent to the physical layer for transmission, they are first encoded with a shortened

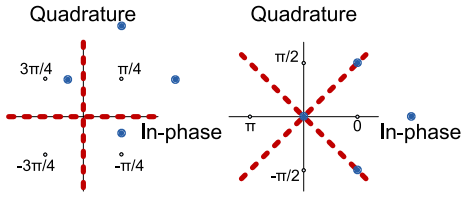



Fig. 2. Constellation diagram of $\pi/4$-DQPSK consists of a set of two signal constellations: QPSK and a $\pi/4$-rotated QPSK. The small dots are the constellation points, the dashed red lines indicate the decision boundaries and the big dots are the constellation points when the $\pi/4$-DQPSK scheme is interfered with a QPSK signal.

Reed Muller code into 30 b and then the resulting 30-b-long stream is scrambled. 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 decodable then both the corresponding uplink subslots shall be regarded as reserved" [12]. Thus, it regards the uplink slot as not available for random access. So according to the protocol it is possible that the mobile will wait indefinitely if it cannot decode the AACH message. From the mobile station point of view it appears that the network is congested, since the devices cannot make new connections, but running conversations are not affected. 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 impedes the system significantly.

## III. Symbol Errors on the Physical Layer Due to Interference Signals

To cause a denial of service, the physical signs of the control messages have to be corrupted. TETRA uses $\pi/4$-DQPSK and the newer versions of TETRA use $\pi/8$-DQPSK and QAM modulation. This research focuses on the widely implemented $\pi/4$-DQPSK modulation. This modulation scheme consists of two signal constellations as shown in Fig. 2 and the modulation scheme switches between these two constellations for every consecutive symbol. In the left constellation, the points lie on $\pi/4$, $3\pi/4$, $-\pi/4$ and $-3\pi/4$. In the right constellation, the points lie on $0$, $\pi/2$, $-\pi$ and $-\pi/2$. The phase transitions between symbols for this modulation scheme are $\pi/4$, $3\pi/4$, $-\pi/4$ and $-3\pi/4$. Disrupting the signal on the physical layer is the obvious choice, since the shared nature of the medium makes it easy to access for interference signals [3].

To achieve errors in the modulation scheme the error vector magnitude (EVM) has to be increased to shift the constellation points over the decision boundaries of both constellations. The EVM is a measure of how much the constellation point is shifted away from the correct position in the constellation diagram.

An asynchronous continuous wave is the simplest signal to create an EVM that shifts the constellation points over the decision boundaries. The data signal superimposed by a continuous wave interference can be described as

$$\begin{aligned} x_n(t) + m(t) = \; & a\cos(\omega t + \phi_n) \\ & + b\cos(\omega t + \Delta\omega t + \phi_m) \end{aligned} \tag{1}$$

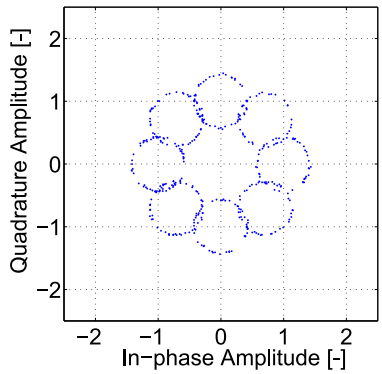



Fig. 3. Constellation diagram of $\pi/4$-DQPSK with continuous wave interference signal. The received constellation points lie on a circle around the ideal points.

where $x_n(t)$ is the data signal, $m(t)$ the interference signal, $a$ the amplitude of the modulated signal, $\omega$ the carrier angular frequency, $t$ the time, $\phi_n$ the modulated phase, $\phi_m$ the phase of the interference signal, and $\Delta\omega$ the difference angular frequency between the modulated signal and the interference signal. The quadrature components of this combined signal can be described as

$$\begin{aligned} I(t) = \; & a\cos(\phi_n) + b\cos(\Delta\omega t + \phi_m) \\ Q(t) = \; & a\sin(\phi_n) + b\sin(\Delta\omega t + \phi_m) \end{aligned} \tag{2}$$

where $I(t)$ is the in-phase component and $Q(t)$ is the quadrature component. The first terms in $I(t)$ and $Q(t)$ are the desired quadrature components of the QPSK signal, and the second terms result from the asynchronous continuous wave interference signal. As a result, the received point in the constellation diagram after demodulation will lie on a circle around the ideal constellation point.

In the same way, a QPSK-modulated interference signal is superposed on the $\pi/4$-DQPSK. In this analysis, the QPSK interference signal is synchronized with the $\pi/4$-DQPSK signal in order to be able to push the points over the decision boundaries as shown in Fig. 2. It is assumed that the signals are exactly synchronized to achieve the clear superposition of the $\pi/4$-DQPSK and the QPSK. In a practical situation, this is never the case. The phase noise and the frequency difference between the interference signal and the modulation signal will rotate the QPSK signal around the $\pi/4$-DQPSK points. In addition, the sampling points to determine the symbols for the $\pi/4$-DQPSK and the QPSK are not in synchronization. Therefore, the QPSK signal will not be sampled on the four points, but also somewhere along the signal trajectory between the four points.

A standard Simulink model has been adapted to determine the effects of interference signals added to the channel [16]. If a continuous wave is added to the channel to interfere with the modulated signal it is expected that the interference signal is superimposed on the original constellation diagram. A QPSK modulated signal is also simulated as an interference signal. Figs. 3, 4, and 5 confirm the superposition of the interference signals as expected by (3). The continuous wave interference signal caused an EVM that rotates around the ideal

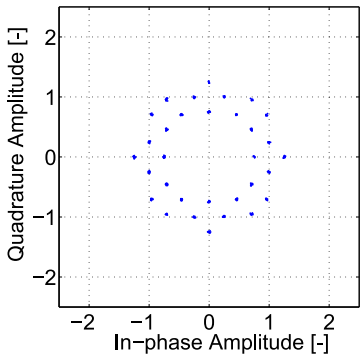



Fig. 4. Constellation diagram of $\pi/4$-DQPSK with a synchronized QPSK interference signal. The QPSK interference signal caused the received points to lie on four points around each ideal constellation point.

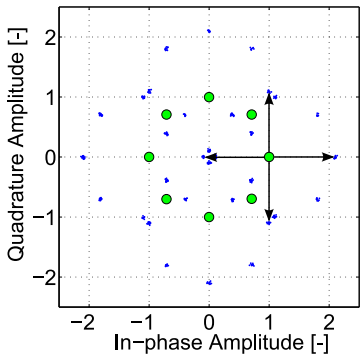



Fig. 5. Constellation diagram of $\pi/4$-DQPSK with large QPSK interference signal. The green points are the ideal $\pi/4$-DQPSK constellation points. The QPSK interference signal causes the received points, which are the blue points, to lie on four points around each ideal constellation point.

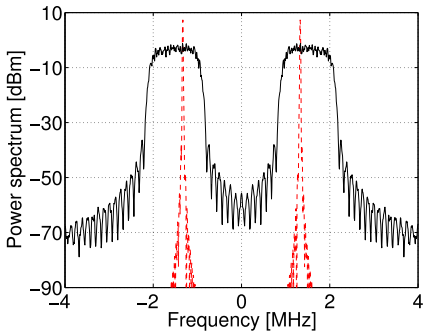



Fig. 6. Spectrum of $\pi/4$-DQPSK (solid black) and continuous wave interference signal (dashed red).

constellation points and the synchronous QPSK-modulated interference signal that caused an EVM consisting four points around the ideal constellation points. Of course, the results in the simulations with the larger amplitudes are not realistic, since in a realistic situation the receiver gets out of synchronization before the results in the simulations are obtained.

The graphs in Figs. 6 and 7 show the spectra of the data signal superimposed by the interference signal. It can be clearly seen that the continuous wave creates a spike in the spectrum, while

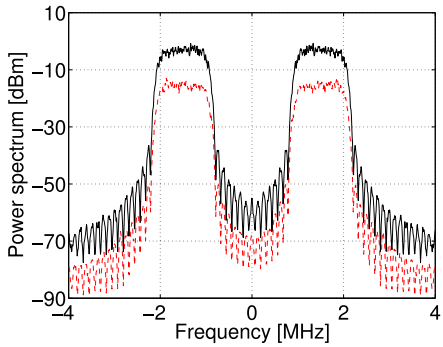



Fig. 7. Spectrum of $\pi/4$-DQPSK (solid black) and QPSK interference signal (dashed red).

the power of the QPSK interference signal is divided over the whole spectrum.

## IV. Intelligent Jammer

A possible threat for a TETRA system would be an intelligent jammer that interferes with the bits involved in AACH control. Jamming these control messages will deny users from service.

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 antijamming techniques [3]. 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 [3], [17]: maximize jamming gain, target jamming, and reduced probability of detection. Intelligent jammers try to exploit protocols in high layers of the OSI model to achieve these goals [3].

In the previous sections, it is shown that the TETRA communication system can be disrupted, so the mobile stations cannot start calls. This is achieved by interfering with the AACH messages sent by the base station, which improves the jamming gain considerably. The probability of detection of the jammer can be reduced by using a QPSK-modulated signal as the interference signal, since the signal is divided over the spectrum as shown in Fig. 7. Furthermore in this case, it is not straightforward to discriminate jamming from the legitimate traffic scenarios using only the signal strength [8]. This discrimination between legitimate and adversarial traffic is also the main challenge for detection of jammers [8].

Other data besides the signal strength are analyzed such as the packet delivery ratio (PDR). Even if a network is congested the PDR always maintains a certain value, while an effective jammer decreases the PDR to a value close to zero [8]. However, this method cannot be applied to detect the jamming attack described in this paper. 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 [8]. 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,

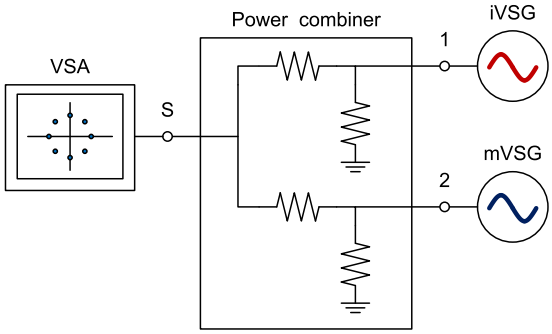



Fig. 8. Measurement setup modulation scheme superposition: an mVSG, an iVSG connected via a power combiner to a VSA.

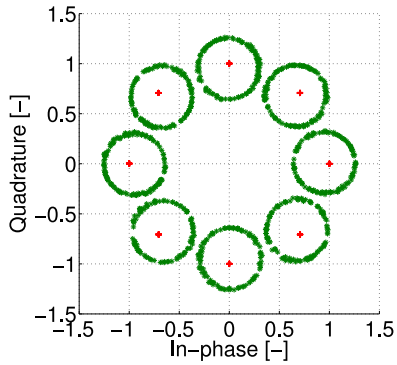



Fig. 9. Constellation diagram without IEMI signal (red pluses); with a synchronized continuous wave IEMI on the centre frequency (blue dots); and with an asynchronous continuous wave IEMI 1000 Hz above the center frequency (green asterisks). The signal with the synchronized continuous wave IEMI on the center frequency lies on top of the signal without IEMI.

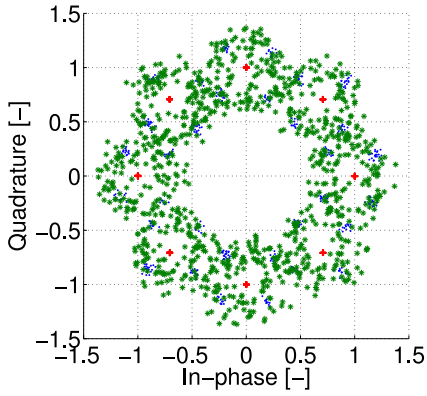



Fig. 10. Constellation diagram without IEMI signal (red pluses); with a synchronized QPSK-modulated IEMI signal on the center frequency (blue dots); and with an asynchronous QPSK-modulated IEMI signal 1000 Hz above the center frequency (green asterisks).

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. An intelligent jammer circumvents this detection, since there is no data for the PDR, because no new conversation can be started and ongoing conversations are not interrupted.

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.

To disrupt the bits a certain jamming-to-signal ratio (JSR) is required. This ratio is given by the following equation [18]:

$$\frac{J}{S} = \frac{P_j G_{jr} G_{rj} R_{tr}^2 L_r B_r}{P_t G_{tr} G_{rt} R_{jr}^2 L_j B_j} \tag{3}$$

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 increases the effectiveness of disrupting the bits. However, it will also increase the possibility of detection.

## V. Experimental Results

In Section III, 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, the concealment of the interference signal and the superposition of the interference signal with the modulated signal are verified.

A vector signal analyzer (VSA) was connected with two vector signal generators (VSG) via a power combiner. The measurement setup shown in Fig. 8 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 minicircuits. The VSA measured the constellation diagram and the spectrum. The following settings were set for the mVSG: center frequency at 390 MHz, power at $-40$ dBm, $\pi/4$-DQPSK modulation, and a symbol rate of 18 kb/s. 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 center frequency and at 1000 Hz above the center frequency of the modulated signal. The iVSG and mVSG were synchronized and unsynchronized by connecting and not connecting the 10-MHz reference signal, respectively. The iVSG sent random bits with QPSK modulation.

The constellation diagrams are shown in Figs. 9 and 10 and the spectra are shown in Figs. 11 and 12. When the continuous wave had the same center frequency and was synchronized via the 10-MHz reference signal with the $\pi/4$-DQPSK signal, 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 Fig. 9. The QPSK signal, however, does create an error and as expected the QPSK signal is superimposed on the $\pi/4$-DQPSK signal. Measurements were performed with larger amplitudes causing the VSA to lose lock on the $\pi/4$-DQPSK

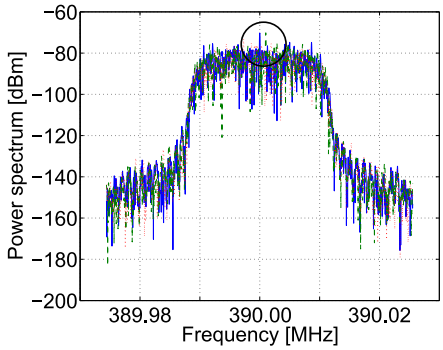



Fig. 11. Spectrum without IEMI signal (dotted red); with a synchronized continuous wave IEMI signal on the center frequency (solid blue); and with an asynchronous continuous wave IEMI 1000 Hz above the center frequency (dashed green).

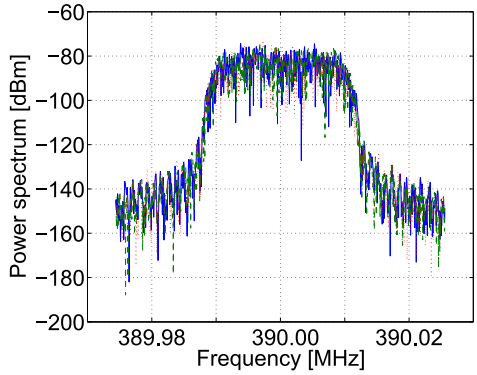



Fig. 12. Spectrum without an IEMI signal (dotted red); with a synchronized QPSK modulated IEMI signal on the center frequency (solid blue); and with an asynchronous QPSK-modulated IEMI signal 1000 Hz above the center frequency (dashed green).

signal and the constellation could not be reconstructed. The EVM readings also increased and varied greatly.

When the continuous wave was unsynchronised and set at 1000 Hz above the center frequency, the constellation rotated, which is in accordance with (3). The asynchrony and setting the frequency 1000 Hz above the center frequency of the $\pi/4$-DQPSK resulted in a cloud of points around the constellation points when a QPSK interference was added. This is because 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 arc. Exact synchronization with the TETRA signal is in practice hard to achieve and therefore the asynchronous results are more realistic.

The continuous wave created a larger EVM than the QPSK signal, however, in Fig. 11, two clear peaks can be seen at the center frequency and 1000 Hz above the center frequency, which are caused by the continuous wave interference. The QPSK interference does not cause a noticeably different spectrum to that shown in Fig. 12. The continuous wave at 1000 Hz above the center frequency caused a larger EVM than the QPSK signal, while also causing a peak in the received spectrum. The QPSK signal, however, did not create a noticeable difference in the received spectrum. The QPSK interference is more difficult to detect than a continuous wave, which is in accordance with the study performed by Mlezcko *et al.* [19], where they show that a signal occupying a significant amount of the bandwidth requires a lower signal level. If the interference signal stays covert, then it is less likely that countermeasures against the interference signal will be taken.

## VI. Conclusion

Terrestrial-trunked radio can be disrupted by an intelligent jammer. The slotted ALOHA protocol can be interfered by corrupting each AACH block, since the terrestrial-trunked radio protocol states that the mobile station will wait indefinitely before transmitting until the AACH can be decoded. The study also showed that an intentional electromagnetic interference 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. Therefore, the TETRA protocol is vulnerable to a QPSK-modulated interference signal corrupting the AACH, since it is hard to detect the interference signal, meaning no countermeasures can be taken against the jammer.

## References

[1] E. Lammerts, C. Slump, and K. Verweij, "Realization of a mobile data application in TETRA," in *Proc. ProRISC Conf.*, Mierlo, The Netherlands, 1999, pp. 247–253.

[2] *Terrestrial Trunked Radio (TETRA): Voice Plus Data (V + D); Designers' Guide; Part 2: Radio Channels, Network Protocols and Service Performance*, ETSI Standard 300 392-2, 1997.

[3] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 2, pp. 245–257, Apr.–Jun. 2011.

[4] (2013). SESP group [Online]. Available: http://www.sesp.com/

[5] (2013). Jammer 4 U cell phone jammer [Online]. Available: http://www.jammer4uk.com/cell-phone-jammer-c-2.html

[6] (2013). WiFi jammer from China [Online]. Available: http://www.jammerfromchina.com/categories/WiFi%7B47%7DBluetooth_jammers/

[7] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. 6th ACM Int. Symp. Mobile ad hoc Netw. Comput.*, 2005, pp. 46–57.

[8] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Netw.*, vol. 20, no. 3, pp. 41–47, May/Jun. 2006.

[9] M. Petracca, M. Vari, F. Vatalaro, and G. Lubello, "Performance evaluation of GSM robustness against smart jamming attacks," in *Proc. 5th Int. Symp. Commun. Control Signal Process.*, 2012, pp. 1–6.

[10] W. D. Prather, C. E. Baum, R. J. Torres, F. Sabath, and D. Nitsch, "Survey of worldwide high-power wideband capabilities," *IEEE Trans. Electromagn. Compat.*, vol. 46, no. 3, pp. 335–344, Aug. 2004.

[11] J. Dunlop, D. Girma, and J. Irvine, *Digital Mobile Communications and the TETRA System*. New York, NY, USA: Wiley, 1999.

[12] *Terrestrial Trunked Radio (TETRA): Voice Plus Data (V + D); Part 2: Air Interface (AI)*, ETSI Standard 300 392-2, 2010.

[13] P. Stavroulakis, *Terrestrial Trunked Radio: TETRA*. New York, NY, USA: Springer, 2007.

[14] J. Mirkovic and P. Reiher, "A taxonomy of ddos attack and ddos defense mechanisms," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–53, 2004.

[15] J. F. Kurose and K. W. Ross, *Computer Networking: A Top Down Approach*. Upper Saddle River, NJ, USA: Addison-Wesley, 2007.

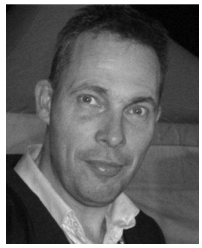
[16] (2013). Simulink passband modulation [Online]. Available: http://www.mathworks.com/help/comm/examples/passband-modulation.html
[17] T. X. Brown, J. E. James, and A. Sethi, "Jamming and sensing of encrypted wireless ad hoc networks," in *Proc. 7th ACM Int. Symp. Mobile ad hoc Netw. Comput.*, 2006, pp. 120–130.
[18] D. C. Schleher, *Electronic Warfare in the Information Age*. Norwood, MA, USA: Artech House, 1999.
[19] M. Mleczko, S. Fisahn, and H. Garbe, "Measurements of EMI signals on radio links based on commercial off-the-shelf wireless devices," in *Proc. Int. Symp. Electromagn. Compat.*, 2012, pp. 1–5.

**Ray R. Tanuhardja** received the B.Sc. and M.Sc. degrees in electrical engineering from the University of Twente, Enschede, The Netherlands, in 2014.

In his graduation project, he investigated the vulnerability of the C2000 communication system used by the emergency services in the Netherlands to intentional electromagnetic interference. In 2014, he was a Guest Researcher with the National Institute of Standards and Technology, Boulder, CO, USA. His research project focused on the characterization of reverberation chambers.

**Stefan van de Beek** (S'13) was born in Voorthuizen, The Netherlands, in March 1988. He received the Masters degree in electrical engineering from the University of Twente, Enschede, The Netherlands, in August 2012. Since September 2012, he has been working toward the Ph.D. degree at the Telecommunication Engineering Group, University of Twente.

His graduation project was performed at the National Institute for Standards and Technologies, Boulder, CO, USA, and focused on characterizing reverberation chambers. He is involved in the project "Strategies for the Improvement of Critical Infrastructure Resilience to Electromagnetic Attacks." His focus is on improving the robustness of wireless mission-critical communication systems against electromagnetic attacks.



**Mark J. Bentum** (S'92–M'95–SM'09) was born in Smilde, The Netherlands, in 1967. He received the M.Sc. degree in electrical engineering from the University of Twente, Enschede, The Netherlands, in August 1991. In December 1995, he received the Ph.D. degree for his thesis "Interactive Visualization of Volume Data" from the same university.

From December 1995 to June 1996, he was a Research Assistant at the University of Twente in the field of signal processing for mobile telecommunications and medical data processing. In June 1996, he joined the Netherlands Foundation for Research in Astronomy (ASTRON). He was in various positions at ASTRON. In 2005, he was involved in the eSMA project in Hawaii to correlate the Dutch JCMT mm-telescope with the submillimeter array of Harvard University. From 2005 to 2008, he was responsible for the construction of the first software radio telescope in the world, low frequency array. In 2008, he became an Associate Professor in the Telecommunication Engineering Group, University of Twente. He is now involved with research and education in mobile radio communications. His current research interests include short-range radio communications, novel receiver technologies (for instance, in the field of radio astronomy), channel modeling, interference mitigation, sensor networks and aerospace. He has acted as a reviewer for various conferences and journals.

Dr. Bentum is Secretary of the Dutch URSI Committee, Initiator and Chair of the IEEE Benelux AES/GRSS Chapter, Board Member of the Dutch Electronics and Radio Society NERG, Member of the Dutch Royal Institute of Engineers KIVI NIRIA, the Dutch Pattern Recognition Society.

**Frank B. J. Leferink** (M'91–SM'08) received the B.Sc degree in 1984, M.Sc. degree in 1992 and the Ph.D. degree in 2001, all in electrical engineering, from the University of Twente, Enschede, The Netherlands.

He has been with THALES, Hengelo, The Netherlands, since 1984, and is currently the Technical Authority EMC. In 2003, he was appointed as (Part-Time, Full Research) Professor, Chair for EMC at the University of Twente. He has published more than 200 peer-reviewed papers. He is an Associate Editor of the IEEE TRANSACTIONS ON EMC.

Dr. Leferink is Chair of the IEEE EMC Benelux Chapter, and a Member of ISC EMC Europe.