

Chapter 1 : A seminar Report On Cell Phone Jammers pdf

Mobile Jammer Seminar and PPT with pdf Report: A mobile phone jammer is an instrument used to prevent cellular phones from receiving signals from base blog.quintoapp.com page contains Mobile Jammer Seminar and PPT with pdf report.

Mobile Jammer A GSM Jammer is a device that transmit signal on the same frequency at which the GSM system operates, the jamming success when the mobile phones in the area where the jammer is located are disabled. Communication jamming devices were first developed and used by military. Where tactical commanders use RF communications to exercise control of their forces, an enemy has interest in those communications. This interest comes from the fundamental area of denying the successful transport of the information from the sender to the receiver. Nowadays the mobile jammer devices are becoming civilian products rather than electronic warfare devices, since with the increasing number of the mobile phone users the need to disable mobile phones in specific places where the ringing of cell phone would be disruptive has increased. These places include worship places, university lecture rooms, libraries, concert halls, meeting rooms, and other places where silence is appreciated. OPERATION Jamming devices overpower the cell phone by transmitting a signal on the same frequency as the cell phone and at a high enough power that the two signals collide and cancel each other out. Cell phones are designed to add power if they experience low-level interference, so the jammer must recognize and match the power increase from the phone. Cell phones are full-duplex devices, which mean they use two separate frequencies, one for talking and one for listening simultaneously. Some jammers block only one of the frequencies used by cell phones, which has the effect of blocking both. The phone is tricked into thinking there is no service because it can receive only one of the frequencies. Less complex devices block only one group of frequencies, while sophisticated jammers can block several types of networks at once to head off dual-mode or tri-mode phones that automatically switch among different network types to find an open signal. Some of the high-end devices block all frequencies at once and others can be tuned to specific frequencies. To jam a cell phone, all you need is a device that broadcasts on the correct frequencies. Although different cellular systems process signals differently, all cell-phone networks use radio signals that can be interrupted. Disrupting a cell phone is the same as jamming any other type of radio communication. A cell phone works by communicating with its service network through a cell tower or base station. Cell towers divide a city into small areas, or cells. As a cell phone user drives down the street, the signal is handed from tower to tower. Mobile Jammer A jamming device transmits on the same radio frequencies as the cell phone, disrupting the communication between the phone and the cell-phone base station in the town. The jammer denies service of the radio spectrum to the cell-phone users within range of the jamming device. Older jammers sometimes were limited to working on phones using only analog or older digital mobile phone standards. Newer models such as the double and triple band jammers can block all widely used systems AMPS, iDEN, GSM, etc and are even very effective against newer phones which hop to different frequencies and systems when interfered with. As the dominant network technology and frequencies used for mobile phones vary worldwide, some work only in specific regions such as Europe or North America. There are concerns that crudely designed jammers may disrupt the functioning of medical devices such as pacemakers. When active in a designated area, such devices will by means of RF interference prevent all pagers and mobile phones located in that area from receiving and transmitting calls. This type of device transmits only a jamming signal and has very poor frequency selectivity, which leads to interference with a larger amount of communication spectrum than it was originally intended to target. One is called brute force jamming, which just blocks everything. The other puts out a small amount of interference, and you could potentially confine it within a single cell block. You could use lots of little pockets of small jamming to keep a facility under control. It has a unique identification number for communicating with the cellular base station. This process of detection and interruption of call establishment is done during the interval normally reserved for signaling and handshaking. These users must pre-register their phone numbers with the service providers. When an incoming call arrives, the detector recognizes that number and the call are

established for a specified maximum duration, say two minutes. The emergency users are also allowed to make out going calls. On leaving the coverage area of the beacon, the handset must re-enable its normal function. Assuming the beacon system uses a technology with its own license or in the license exempt band , no change to the regulations are needed to deploy such a system. The jammer is predominantly in receiving mode and will intelligently choose to interact and block the cell phone directly if it is within close proximity of the jammer. This selective jamming technique uses a discriminating receiver to target the jamming transmitter. The benefit of such targeting selectivity is much less electromagnetic pollution in terms of raw power transmitted and frequency spectrum from the jammer, and therefore much less disruptive to passing traffic. The jam signal would only stay on as long as the mobile continues to make a link with the base station, otherwise there would be no jamming transmission – the technique forces the link to break or unhook and then it retreats to a passive receive mode again. This technique has an added advantage over Type B in that no added overhead time or effort is spent negotiating with the cellular network. Although labor intensive to construct, the Faraday cage essentially blocks, or greatly attenuates, virtually all electromagnetic radiation from entering or leaving the cage – or in this case a target room. Emergency calls would be blocked unless there was a way to receive and decode the transmissions, pass by coax outside the room and re-transmitted. This passive configuration is currently legal in Canada for any commercial or residential location insofar as DOC Industry Canada is concerned, however municipal or provincial building code by- laws may or may not allow this type of construction. CONCLUSION This project is mainly intended to prevent the usage of mobile phones in places inside its coverage without interfering with the communication channels outside its range, thus providing a cheap and reliable method for blocking mobile communication in the required restricted areas only. Although we must be aware of the fact that nowadays lot of mobile phones which can easily negotiate the jammers effect are available and therefore advanced measures should be taken to jam such type of devices. These jammers includes the intelligent jammers which directly communicates with the GSM provider to block the services to the clients in the restricted areas, but we need the support from the providers for this purpose.

Chapter 2 : Download the Seminar Report for Cell Phone Jammer

A seminar Report On Cell Phone Jammers Cell Phone blog.quintoapp.com (Size: KB / Downloads:) INTRODUCTION
Cell phones are everywhere these days. According to the Cellular Telecommunications and Internet Association, almost million people in the United States had cell-phone service in January

Sunday, June 28 Cell Phone Jammer: Communication jamming devices were first developed and used by military. Where tactical commanders use RF communications to exercise control of their forces, an enemy has interest in those communications. This interest comes from the fundamental area of denying the successful transport of the information from the sender to the receiver. Nowadays the mobile jammer devices or cell phone jammer software are becoming civilian products rather than electronic warfare devices, since with the increasing number of the mobile phone users the need to disable mobile phones in specific places where the ringing of cell phone would be disruptive has increased. These places include worship places, university lecture rooms, libraries, concert halls, meeting rooms, and other places where silence is appreciated. Construction of Mobile Jammer Jamming devices overpower the cell phone by transmitting a signal on the same frequency as the cell phone and at a high enough power that the two signals collide and cancel each other out. Cell phones are designed to add power if they experience low-level interference, so the jammer must recognize and match the power increase from the phone. Cell phones are full-duplex devices, which mean they use two separate frequencies, one for talking and one for listening simultaneously. Some jammers block only one of the frequencies used by cell phones, which has the effect of blocking both. The phone is tricked into thinking there is no service because it can receive only one of the frequencies. Less complex devices block only one group of frequencies, while sophisticated jammers can block several types of networks at once to head off dual-mode or tri-mode phones that automatically switch among different network types to find an open signal. Some of the high-end devices block all frequencies at once and others can be tuned to specific frequencies. To jam a cell phone, all you need is a device that broadcasts on the correct frequencies. Although different cellular systems process signals differently, all cell-phone networks use radio signals that can be interrupted. Disrupting a cell phone is the same as jamming any other type of radio communication. A cell phone works by communicating with its service network through a cell tower or base station. Cell towers divide a city into small areas, or cells. The jammer denies service of the radio spectrum to the cell-phone users within range of the jamming device. Older jammers sometimes were limited to working on phones using only analog or older digital mobile phone standards. Newer models such as the double and triple band jammers can block all widely used systems AMPS, iDEN, GSM, etc and are even very effective against newer phones which hop to different frequencies and systems when interfered with. As the dominant network technology and frequencies used for mobile phones vary worldwide, some work only in specific regions such as Europe or North America. There are concerns that crudely designed jammers may disrupt the functioning of medical devices such as pacemakers. When active in a designated area, such devices will by means of RF interference prevent all pagers and mobile phones located in that area from receiving and transmitting calls. This type of device transmits only a jamming signal and has very poor frequency selectivity, which leads to interference with a larger amount of communication spectrum than it was originally intended to target. One is called brute force jamming, which just blocks everything. The other puts out a small amount of interference, and you could potentially confine it within a single cell block. You could use lots of little pockets of small jamming to keep a facility under control. It has a unique identification number for communicating with the cellular base station. This process of detection and interruption of call establishment is done during the interval normally reserved for signaling and handshaking. These users must pre-register their phone numbers with the service providers. When an incoming call arrives, the detector recognizes that number and the call are established for a specified maximum duration, say two minutes. The emergency users are also allowed to make out going calls.

Chapter 3 : seminar ppt of mobile jammer

A GSM Jammer or cell phone jammer is a device that transmit signal on the same frequency at which the GSM system operates, the jamming success when the mobile phones in the area where the jammer is located are disabled.

It provides a valuable service to its users who are willing to pay a considerable premium over a fixed line phone, to be able to walk and talk freely. Because of its usefulness and the money involved in the business, it is subject to fraud. Unfortunately, the advance of security standards has not kept pace with the dissemination of mobile communication. Some of the features of mobile communication make it an alluring target for criminals. It is a relatively new invention, so not all people are quite familiar with its possibilities, in good or in bad. Its newness also means intense competition among mobile phone service providers as they are attracting customers. The major threat to mobile phone is from cloning. Cell phone cloning is copying the identity of one mobile telephone to another mobile telephone. Usually this is done for the purpose of making fraudulent telephone calls. The bills for the calls go to the legitimate subscriber. The cloner is also able to make effectively anonymous calls, which attracts another group of interested users. Cloning is the process of taking the programmed information that is stored in a legitimate mobile phone and illegally programming the identical information into another mobile phone. The result is that the "cloned" phone can make and receive calls and the charges for those calls are billed to the legitimate subscriber. The service provider network does not have a way to differentiate between the legitimate phone and the "cloned" phone. The early s were boom times for eavesdroppers. A method for transmitting simultaneous signals over a shared portion of the spectrum. The answer is yes. In spite of this, the security functions which prevent eavesdropping and Unauthorized uses are emphasized by the mobile phone companies. The existing mobile communication networks are not safer than the fixed Telephone networks. They only offer protection against the new forms of abuse. The following functions exist: Some subscribers of Reliance had to suffer because their phone was cloned. Mobile Cloning Is in initial stages in India so preventive steps should be taken by the network provider and the Government. Cloning has been successfully demonstrated under GSM, but the process is not easy and it currently remains in the realm of serious hobbyists and researchers. Too many users treat their mobile phones as gadgets rather than as business assets covered by corporate security policy. This is possible because Sims are not network specific and, though tamper-proof, their security is flawed. In fact, a Sim can be cloned many times and the resulting cards used in numerous phones, each feeding illegally off the same bill. But there are locking mechanisms on the cellular phones that require a PIN to access the phone. This would dissuade some attackers, foil others, but might not work against a well financed and equipped attacker. An 8-digit PIN requires approximately 50,, guesses, but there may be ways for sophisticated attackers to bypass it. Mobile phones, they say, are secure and privacy friendly. This is not entirely true. While the amateur scanner menace has been largely exterminated, there is now more potential than ever before for privacy invasion. The alleged security of GSM relies on the myth that encryption - the mathematical scrambling of our conversations - makes it impossible for anyone to intercept and understand our words. And while this claim looks good on paper, it does not stand up to scrutiny. The reality is that the encryption has deliberately been made insecure. Many encrypted calls can therefore be intercepted and decrypted with a laptop computer. This number is loaded when the phone number is manufactured. This is a unique number. Which is used to clone CDMA phones. Patagonia is software available in the market which is used to clone CDMA phone. Using this software a cloner can take over the control of a CDMA phone i. A SIM can be cloned again and again and they can be used at different places. Messages and calls sent by cloned phones can be tracked. Authentication allows the mobile service provider network to determine the legitimacy of a mobile phone. Phones determined to be "clones" can be instantly denied access to service before any calls are made or received. Frequent wrong number phone calls to your phone, or hang-ups. Difficulty in placing outgoing calls. Difficulty in retrieving voice mail messages. Incoming calls constantly receiving busy signals or wrong numbers. Messages and calls can track sent by cloned phones. The MIN often can be dialed from other wireless or wire line networks. The number differs from the electronic serial number ESN , which is the unit number assigned by a phone

manufacturer. Check that all mobile devices are covered by a corporate security policy. Ensure one person is responsible for keeping tabs on who has what equipment and that they update the central register. How do service providers handle reports of cloned phones? Typically, the service provider will assume the cost of those additional fraudulent calls. However, to keep the cloned phone from continuing to receive service, the service provider will terminate the legitimate phone subscription. Authentication is a mathematical process by which identical calculations are performed in both the network and the mobile phone. These calculations use secret information known as a "key" preprogrammed into both the mobile phone and the network before service is activated. Cloners typically have no access to this secret information. A legitimate mobile phone will produce the same calculated result as the network. If they match, the phone is not a "clone. Yes, for the most part. However, Authentication is the most robust and reliable method for preventing cloning fraud and it is the only industry "standard" method for eliminating cloning. The fact that it is standardized means that all mobile telecommunications networks using IS can support Authentication. There is no need to add proprietary equipment, software, or communications protocols to the networks to prevent cloning fraud. Otherwise, it depends on how old the phone is and the make and model. Almost all phones manufactured since the beginning of support the Authentication function. They are using many methods such as RF Fingerprinting, subscriber behavior profiling, and Authentication. RF Fingerprinting is a method to uniquely identify mobile phones based on certain unique radio frequency transmission characteristics that are essentially "fingerprints" of the radio being used. Subscriber behavior profiling is used to predict possible fraudulent use of mobile service based on the types of calls previously made by the subscriber. Authentication has advantages over these technologies in that it is the only industry standardized procedure that is transparent to the user, a technology that can effectively combat roamer fraud, and is a prevention system as opposed to a detection system. IS Interim Standard No. IS is the standard that defines the methods for automatic roaming, handoff between systems, and for performing Authentication. With technically sophisticated thieves, customers are relatively helpless against cellular phone fraud. Usually they became aware of the fraud only once receiving their phone bill. Service providers have adopted certain measures to prevent cellular fraud. These include encryption, blocking, blacklisting, user verification and traffic analysis: Blocking is used by service providers to protect themselves from high risk callers. For example, international calls can be made only with prior approval. In some countries only users with major credit cards and good credit ratings are allowed to make long distance calls. An Equipment Identity Register EIR enables network operators to disable stolen cellular phones on networks around the world. Other warning signs that subscribers should watch out for to detect fraudulent activity include: Mobile Cloning Is in initial stages in India so preventive steps should be taken by the network provider and the Government the enactment of legislation to prosecute crimes related to cellular phones is not viewed as a priority, however. It is essential that intended mobile crime legislation be comprehensive enough to incorporate cellular phone fraud, in particular "cloning fraud" as a specific crime.

Chapter 4 : September |Seminar PPT-Slides-Report-Topics-PDF-DOC-Free Download

*Are you interested in any one of the topics. Then mail to us immediately for more assistance!!!
"seminaronly@blog.quintoapp.com" Thank you for choosing blog.quintoapp.com*

Communication jamming devices were first developed and used by military. Where tactical commanders use RF communications to exercise control of their forces, an enemy has interest in those communications. This interest comes from the fundamental area of denying the successful transport of the information from the sender to the receiver. Nowadays the mobile jammer devices or cell phone jammer software are becoming civilian products rather than electronic warfare devices, since with the increasing number of the mobile phone users the need to disable mobile phones in specific places where the ringing of cell phone would be disruptive has increased. These places include worship places, university lecture rooms, libraries, concert halls, meeting rooms, and other places where silence is appreciated. Introduction of Mobile Jammer Jamming devices overpower the cell phone by transmitting a signal on the same frequency as the cell phone and at a high enough power that the two signals collide and cancel each other out. Cell phones are designed to add power if they experience low-level interference, so the jammer must recognize and match the power increase from the phone. Cell phones are full-duplex devices, which mean they use two separate frequencies, one for talking and one for listening simultaneously. Some jammers block only one of the frequencies used by cell phones, which has the effect of blocking both. The phone is tricked into thinking there is no service because it can receive only one of the frequencies. Less complex devices block only one group of frequencies, while sophisticated jammers can block several types of networks at once to head off dual-mode or tri-mode phones that automatically switch among different network types to find an open signal. Some of the high-end devices block all frequencies at once and others can be tuned to specific frequencies. To jam a cell phone, all you need is a device that broadcasts on the correct frequencies. Although different cellular systems process signals differently, all cell-phone networks use radio signals that can be interrupted. Disrupting a cell phone is the same as jamming any other type of radio communication. A cell phone works by communicating with its service network through a cell tower or base station. Cell towers divide a city into small areas, or cells. The jammer denies service of the radio spectrum to the cell-phone users within range of the jamming device. Older jammers sometimes were limited to working on phones using only analog or older digital mobile phone standards. Newer models such as the double and triple band jammers can block all widely used systems AMPS, iDEN, GSM, etc and are even very effective against newer phones which hop to different frequencies and systems when interfered with. As the dominant network technology and frequencies used for mobile phones vary worldwide, some work only in specific regions such as Europe or North America. There are concerns that crudely designed jammers may disrupt the functioning of medical devices such as pacemakers. When active in a designated area, such devices will by means of RF interference prevent all pagers and mobile phones located in that area from receiving and transmitting calls. This type of device transmits only a jamming signal and has very poor frequency selectivity, which leads to interference with a larger amount of communication spectrum than it was originally intended to target. Technologist Jim Mahan said, "There are two types. One is called brute force jamming, which just blocks everything. The other puts out a small amount of interference, and you could potentially confine it within a single cell block. You could use lots of little pockets of small jamming to keep a facility under control. It has a unique identification number for communicating with the cellular base station. This process of detection and interruption of call establishment is done during the interval normally reserved for signaling and handshaking. These users must pre-register their phone numbers with the service providers. When an incoming call arrives, the detector recognizes that number and the call are established for a specified maximum duration, say two minutes. The emergency users are also allowed to make out going calls. Similarly, the system is capable of recognizing and allowing all emergency calls routed to "". Are you interested in this topic. Then mail to us immediately to get the full report.

Chapter 5 : Mobile Jammer|Seminar PPT-Slides-Report-Topics-PDF-DOC-Free Download

Cell Phone Jammers Seminar Report' 06 ABSTRACT Radiation in cell phones is generated in the transmitter and emitted through the antenna. Cell phones have low-power transmitters in them.

Tech Engineering for the year , and Mobile Jammer A GSM Jammer is a device that transmit signal on the same frequency at which the GSM system operates, the jamming success when the mobile phones in the area where the jammer is located are disabled. Communication jamming devices were first developed and used by military. Where tactical commanders use RF communications to exercise control of their forces, an enemy has interest in those communications. This interest comes from the fundamental area of denying the successful transport of the information from the sender to the receiver. Nowadays the mobile jammer devices are becoming civilian products rather than electronic warfare devices, since with the increasing number of the mobile phone users the need to disable mobile phones in specific places where the ringing of cell phone would be disruptive has increased. These places include worship places, university lecture rooms, libraries, concert halls, meeting rooms, and other places where silence is appreciated. OPERATION Jamming devices overpower the cell phone by transmitting a signal on the same frequency as the cell phone and at a high enough power that the two signals collide and cancel each other out. Cell phones are designed to add power if they experience low-level interference, so the jammer must recognize and match the power increase from the phone. Cell phones are full-duplex devices, which mean they use two separate frequencies, one for talking and one for listening simultaneously. Some jammers block only one of the frequencies used by cell phones, which has the effect of blocking both. The phone is tricked into thinking there is no service because it can receive only one of the frequencies. Less complex devices block only one group of frequencies, while sophisticated jammers can block several types of networks at once to head off dual-mode or tri-mode phones that automatically switch among different network types to find an open signal. Some of the high-end devices block all frequencies at once and others can be tuned to specific frequencies. To jam a cell phone, all you need is a device that broadcasts on the correct frequencies. Although different cellular systems process signals differently, all cell-phone networks use radio signals that can be interrupted. Disrupting a cell phone is the same as jamming any other type of radio communication. A cell phone works by communicating with its service network through a cell tower or base station. Cell towers divide a city into small areas, or cells. As a cell phone user drives down the street, the signal is handed from tower to tower. Mobile Jammer A jamming device transmits on the same radio frequencies as the cell phone, disrupting the communication between the phone and the cell-phone base station in the town. The jammer denies service of the radio spectrum to the cell-phone users within range of the jamming device. Older jammers sometimes were limited to working on phones using only analog or older digital mobile phone standards. Newer models such as the double and triple band jammers can block all widely used systems AMPS, iDEN, GSM, etc and are even very effective against newer phones which hop to different frequencies and systems when interfered with. As the dominant network technology and frequencies used for mobile phones vary worldwide, some work only in specific regions such as Europe or North America. There are concerns that crudely designed jammers may disrupt the functioning of medical devices such as pacemakers. When active in a designated area, such devices will by means of RF interference prevent all pagers and mobile phones located in that area from receiving and transmitting calls. This type of device transmits only a jamming signal and has very poor frequency selectivity, which leads to interference with a larger amount of communication spectrum than it was originally intended to target. One is called brute force jamming, which just blocks everything. The other puts out a small amount of interference, and you could potentially confine it within a single cell block. You could use lots of little pockets of small jamming to keep a facility under control. It has a unique identification number for communicating with the cellular base station. This process of detection and interruption of call establishment is done during the interval normally reserved for signaling and handshaking. These users must pre-register their phone numbers with the service providers. When an incoming call arrives, the detector recognizes that number and the call are established for a specified maximum duration, say two minutes. The emergency users are also allowed to

make out going calls. On leaving the coverage area of the beacon, the handset must re-enable its normal function. Assuming the beacon system uses a technology with its own license or in the license exempt band , no change to the regulations are needed to deploy such a system. The jammer is predominantly in receiving mode and will intelligently choose to interact and block the cell phone directly if it is within close proximity of the jammer. This selective jamming technique uses a discriminating receiver to target the jamming transmitter. The benefit of such targeting selectivity is much less electromagnetic pollution in terms of raw power transmitted and frequency spectrum from the jammer, and therefore much less disruptive to passing traffic. The jam signal would only stay on as long as the mobile continues to make a link with the base station, otherwise there would be no jamming transmission – the technique forces the link to break or unhook and then it retreats to a passive receive mode again. This technique has an added advantage over Type B in that no added overhead time or effort is spent negotiating with the cellular network. Although labor intensive to construct, the Faraday cage essentially blocks, or greatly attenuates, virtually all electromagnetic radiation from entering or leaving the cage – or in this case a target room. Emergency calls would be blocked unless there was a way to receive and decode the transmissions, pass by coax outside the room and re-transmitted. This passive configuration is currently legal in Canada for any commercial or residential location insofar as DOC Industry Canada is concerned, however municipal or provincial building code by- laws may or may not allow this type of construction. CONCLUSION This project is mainly intended to prevent the usage of mobile phones in places inside its coverage without interfering with the communication channels outside its range, thus providing a cheap and reliable method for blocking mobile communication in the required restricted areas only. Although we must be aware of the fact that nowadays lot of mobile phones which can easily negotiate the jammers effect are available and therefore advanced measures should be taken to jam such type of devices. These jammers includes the intelligent jammers which directly communicates with the GSM provider to block the services to the clients in the restricted areas, but we need the support from the providers for this purpose.

Chapter 6 : Mobile jammer Brant - a-spy mobile jammer seminar

Cell Phone Jammer, Ask Latest information, Abstract, Report, Presentation (pdf, doc, ppt), Cell Phone Jammer technology discussion, Cell Phone Jammer paper presentation details.

Published on July 16, Abstract A GSM Jammer or cell phone jammer is a device that transmit signal on the same frequency at which the GSM system operates, the jamming success when the mobile phones in the area where the jammer is located are disabled. Communication jamming devices were first developed and used by military. Where tactical commanders use RF communications to exercise control of their forces, an enemy has interest in those communications. This interest comes from the fundamental area of denying the successful transport of the information from the sender to the receiver. Nowadays the mobile jammer devices or cell phone jammer software are becoming civilian products rather than electronic warfare devices, since with the increasing number of the mobile phone users the need to disable mobile phones in specific places where the ringing of cell phone would be disruptive has increased. These places include worship places, university lecture rooms, libraries, concert halls, meeting rooms, and other places where silence is appreciated. Introduction of Mobile Jammer Jamming devices overpower the cell phone by transmitting a signal on the same frequency as the cell phone and at a high enough power that the two signals collide and cancel each other out. Cell phones are designed to add power if they experience low-level interference, so the jammer must recognize and match the power increase from the phone. Cell phones are full-duplex devices, which mean they use two separate frequencies, one for talking and one for listening simultaneously. Some jammers block only one of the frequencies used by cell phones, which has the effect of blocking both. The phone is tricked into thinking there is no service because it can receive only one of the frequencies. Less complex devices block only one group of frequencies, while sophisticated jammers can block several types of networks at once to head off dual-mode or tri-mode phones that automatically switch among different network types to find an open signal. Some of the high-end devices block all frequencies at once and others can be tuned to specific frequencies. To jam a cell phone, all you need is a device that broadcasts on the correct frequencies. Although different cellular systems process signals differently, all cell-phone networks use radio signals that can be interrupted. Disrupting a cell phone is the same as jamming any other type of radio communication. A cell phone works by communicating with its service network through a cell tower or base station. Cell towers divide a city into small areas, or cells. The jammer denies service of the radio spectrum to the cell-phone users within range of the jamming device. Older jammers sometimes were limited to working on phones using only analog or older digital mobile phone standards. Newer models such as the double and triple band jammers can block all widely used systems AMPS, iDEN, GSM, etc and are even very effective against newer phones which hop to different frequencies and systems when interfered with. As the dominant network technology and frequencies used for mobile phones vary worldwide, some work only in specific regions such as Europe or North America. There are concerns that crudely designed jammers may disrupt the functioning of medical devices such as pacemakers. When active in a designated area, such devices will by means of RF interference prevent all pagers and mobile phones located in that area from receiving and transmitting calls. This type of device transmits only a jamming signal and has very poor frequency selectivity, which leads to interference with a larger amount of communication spectrum than it was originally intended to target. Technologist Jim Mahan said, "There are two types. One is called brute force jamming, which just blocks everything. The other puts out a small amount of interference, and you could potentially confine it within a single cell block. You could use lots of little pockets of small jamming to keep a facility under control. It has a unique identification number for communicating with the cellular base station. This process of detection and interruption of call establishment is done during the interval normally reserved for signaling and handshaking. These users must pre-register their phone numbers with the service providers. When an incoming call arrives, the detector recognizes that number and the call are established for a specified maximum duration, say two minutes. The emergency users are also allowed to make out going calls. Similarly, the system is capable of recognizing and allowing all emergency calls routed to "". On leaving the coverage area of the beacon, the handset must

re-enable its normal function. Assuming the beacon system uses a technology with its own license or in the license exempt band , no change to the regulations are needed to deploy such a system. The jammer is predominantly in receiving mode and will intelligently choose to interact and block the cell phone directly if it is within close proximity of the jammer. This selective jamming technique uses a discriminating receiver to target the jamming transmitter. The benefit of such targeting selectivity is much less electromagnetic pollution in terms of raw power transmitted and frequency spectrum from the jammer, and therefore much less disruptive to passing traffic. The jam signal would only stay on as long as the mobile continues to make a link with the base station, otherwise there would be no jamming transmission – the technique forces the link to break or unhook and then it retreats to a passive receive mode again. This technique has an added advantage over Type B in that no added overhead time or effort is spent negotiating with the cellular network. Although labor intensive to construct, the Faraday cage essentially blocks, or greatly attenuates, virtually all electromagnetic radiation from entering or leaving the cage – or in this case a target room. Emergency calls would be blocked unless there was a way to receive and decode the transmissions, pass by coax outside the room and re-transmitted. This passive configuration is currently legal in Canada for any commercial or residential location insofar as DOC Industry Canada is concerned, however municipal or provincial building code by- laws may or may not allow this type of construction. **CONCLUSION** This project is mainly intended to prevent the usage of mobile phones in places inside its coverage without interfering with the communication channels outside its range, thus providing a cheap and reliable method for blocking mobile communication in the required restricted areas only. Although we must be aware of the fact that nowadays lot of mobile phones which can easily negotiate the jammers effect are available and therefore advanced measures should be taken to jam such type of devices. These jammers includes the intelligent jammers which directly communicates with the GSM provider to block the services to the clients in the restricted areas, but we need the support from the providers for this purpose. Next More Seminar Topics: Are you interested in this topic. Then mail to us immediately to get the full report.

Chapter 7 : Cell Phone Jammer Seminar Abstract | Seminar Report,PPT,PDF,DOC,Presentation,Free Dow

Get More Information about Cell Phone Jammer PDF by visiting this link. GSM Jammer or cell phone jammer is a device that transmit signal on the same frequency at which the GSM system operates, the jamming success when the mobile phones in the area where the jammer is located are disabled.

When used, the jammer effectively disables cellular phones. These devices can be used in practically any location, but are found primarily in places where a phone call would be particularly disruptive because silence is expected. Cell phone jammers block cell phone use by sending out radio waves along the same frequencies that cellular phones use. This causes enough interference with the communication between cell phones and towers to render the phones unusable. It transmits low power radio signals to cut off communication between cell phone and cellular base stations. All the mobile phone have the specified radio frequency under which they are operating. Phone jammers interfere with the working frequency of the mobile phone and results in noisy and interference frequency. In this way cell phone jammers block cell phone use by sending out radio waves along the same frequencies that cellular phones use as described above. This causes plenty of interference with the communication between cell phones and signal generated from the mobile towers. Most cell phones use different bands to send and receive communications from towers called full duplexing. Jammers can work by either disrupting phone to tower frequencies or tower to phone frequencies. Smaller handheld models block all bands from MHz to MHz within a 30 foot range 9 meters. Small instruments tend to use the former method, while larger more costly models may interfere directly with the tower. The radius of cell phone jammers can range from a dozen feet for pocket models to kilometers for more dedicated units. The TRJ jammer can block cellular communications for a 5-mile 8 km radius. Their are several types of duplexing like single duplexing , double duplexing mode and multiple duplexing. Duplexing basically defines the transfer of signal voice signal in a manner. These manner are defined from the way of duplexing. Hence duplexing can carry out the jamming of voice signals. You could replace the chip with an electret microphone and listen to yourself talk on a scanner, so the unit could easily couple as a UHF Bug.

Chapter 8 : How to Make A Cell Phone Jammer

Seminar Topics on Cellphone Jammers blog.quintoapp.com

According to the Cellular Telecommunications and Internet Association, almost million people in the United States had cell-phone service in January And cell phones are even more ubiquitous in Europe. Unfortunately, restaurants, movie theaters, concerts, shopping malls and churches all suffer from the spread of cell phones because not all cell-phone users know when to stop talking. While most of us just grumble and move on, some people are actually going to extremes to retaliate. Cell phones are basically handheld two-way radios. And like any radio, the signal can be disrupted, or jammed. Cell towers divide a city into small areas, or cells. As a cell-phone user drives down the street, the signal is handed from tower to tower

HOW IT WORKS

Jamming devices overpower the cell phone by transmitting a signal on the same frequency and at a high enough power that the two signals collide and cancel each other out. Cell phones are designed to add power if they experience low-level interference, so the jammer must recognize and match the power increase from the phone. Cell phones are full-duplex devices, which means they use two separate frequencies, one for talking and one for listening simultaneously. Some jammers block only one of the frequencies used by cell phones, which has the effect of blocking both. The phone is tricked into thinking there is no service because it can receive only one of the frequencies. Less complex devices block only one group of frequencies, while sophisticated jammers can block several types of networks at once to head off dual-mode or tri-mode phones that automatically switch among different network types to find an open signal. Some of the high-end devices block all frequencies at once, and others can be tuned to specific frequencies. To jam a cell phone, all you need is a device that broadcasts on the correct frequencies. Although different cellular systems process signals differently, all cell-phone networks use radio signals that can be interrupted. The bombs that blew up commuter trains in Spain in March , as well as blasts in Bali in October and Jakarta in August , all relied on cell phones to trigger explosives. It has been widely reported that a cell-phone jammer thwarted an assassination attempt on Pakistani President Musharraf in December During a hostage situation, police can control when and where a captor can make a phone call. Cell-phone jammers can be used in areas where radio transmissions are dangerous, such as areas with a potentially explosive atmosphere, such as chemical storage facilities or grain elevators. In the United States, cell-phone jamming is covered under the Communications Act of , which prohibits people from "willfully or maliciously interfering with the radio communications of any station licensed or authorized" to operate. In fact, the "manufacture, importation, sale or offer for sale, including advertising, of devices designed to block or jam wireless transmissions is prohibited" as well. Jamming is seen as property theft, because a private company has purchased the rights to the radio spectrum, and jamming the spectrum is akin to stealing the property the company has purchased. It also represents a safety hazard because jamming blocks all calls in the area, not just the annoying ones. Jamming a signal could block the call of a babysitter frantically trying to contact a parent or a some one trying to call for an ambulance. The Federal Communications Commission is charged with enforcing jamming laws. However, the agency has not yet prosecuted anyone for cell-phone jamming. That means using things like wallpaper or building materials embedded with metal fragments to prevent cell-phone signals from reaching inside or outside the room. Some buildings have designs that block radio signals by accident due to thick concrete walls or a steel skeleton. Companies are working on devices that control a cell phone but do not "jam the signal. The argument is that the phone still works, so it is technically not being jammed. It is a legal gray area that has not been ruled on by the FCC as of April Cell-phone alerters are available that indicate the presence of a cell-phone signal. These have been used in hospitals where cell-phone signals could interfere with sensitive medical equipment. When a signal is detected, users are asked to turn off their phones. You can flip on a CB radio and receive 40 more. You can flip on a TV and receive numerous broadcast channels. Cell phones can send and receive hundreds of frequencies. And this is just the tip of the radio spectrum iceberg. Literally tens of thousands of other radio broadcasts and conversations are zipping past you as you read this article -- police officers, firefighters, ambulance drivers, paramedics, sanitation workers, space shuttle astronauts, race car

drivers, and even babies with their monitors are transmitting radio waves all around you at this very moment! To tap into this ocean of electromagnetic dialog and hear what all of these people are talking about, all you need is a scanner. A scanner is basically a radio receiver capable of receiving multiple signals.

Chapter 9 : Mobile Jammer Seminar Report with PPT and PDF

Seminar Report & Project Report (PPT,PDF,DOC,ZIP) cell phone jammer incorporated with cell phone detector seminars report. Guest Thinking To Register #1.

Published on Nov 14, Abstract A GSM Jammer or cell phone jammer is a device that transmit signal on the same frequency at which the GSM system operates, the jamming success when the mobile phones in the area where the jammer is located are disabled. Communication jamming devices were first developed and used by military. Where tactical commanders use RF communications to exercise control of their forces, an enemy has interest in those communications. This interest comes from the fundamental area of denying the successful transport of the information from the sender to the receiver. Nowadays the mobile jammer devices or cell phone jammer software are becoming civilian products rather than electronic warfare devices, since with the increasing number of the mobile phone users the need to disable mobile phones in specific places where the ringing of cell phone would be disruptive has increased. These places include worship places, university lecture rooms, libraries, concert halls, meeting rooms, and other places where silence is appreciated

Introduction of GSM Mobile Jammer Jamming devices overpower the cell phone by transmitting a signal on the same frequency as the cell phone and at a high enough power that the two signals collide and cancel each other out. Cell phones are designed to add power if they experience low-level interference, so the jammer must recognize and match the power increase from the phone. Cell phones are full-duplex devices, which mean they use two separate frequencies, one for talking and one for listening simultaneously. Some jammers block only one of the frequencies used by cell phones, which has the effect of blocking both. The phone is tricked into thinking there is no service because it can receive only one of the frequencies. Less complex devices block only one group of frequencies, while sophisticated jammers can block several types of networks at once to head off dual-mode or tri-mode phones that automatically switch among different network types to find an open signal. Some of the high-end devices block all frequencies at once and others can be tuned to specific frequencies. To jam a cell phone, all you need is a device that broadcasts on the correct frequencies. Although different cellular systems process signals differently, all cell-phone networks use radio signals that can be interrupted. Disrupting a cell phone is the same as jamming any other type of radio communication. A cell phone works by communicating with its service network through a cell tower or base station. Cell towers divide a city into small areas, or cells. The jammer denies service of the radio spectrum to the cell-phone users within range of the jamming device. Older jammers sometimes were limited to working on phones using only analog or older digital mobile phone standards. Newer models such as the double and triple band jammers can block all widely used systems AMPS, iDEN, GSM, etc and are even very effective against newer phones which hop to different frequencies and systems when interfered with. As the dominant network technology and frequencies used for mobile phones vary worldwide, some work only in specific regions such as Europe or North America. There are concerns that crudely designed jammers may disrupt the functioning of medical devices such as pacemakers. When active in a designated area, such devices will by means of RF interference prevent all pagers and mobile phones located in that area from receiving and transmitting calls. This type of device transmits only a jamming signal and has very poor frequency selectivity, which leads to interference with a larger amount of communication spectrum than it was originally intended to target. Technologist Jim Mahan said, "There are two types. One is called brute force jamming, which just blocks everything. The other puts out a small amount of interference, and you could potentially confine it within a single cell block. You could use lots of little pockets of small jamming to keep a facility under control. It has a unique identification number for communicating with the cellular base station. This process of detection and interruption of call establishment is done during the interval normally reserved for signaling and handshaking. These users must pre-register their phone numbers with the service providers. When an incoming call arrives, the detector recognizes that number and the call are established for a specified maximum duration, say two minutes. The emergency users are also allowed to make out going calls. Similarly, the system is capable of recognizing and allowing all emergency calls routed to "".