Artículos originales

Modelo de Red seguro para M-Learning en cárceles del sistema penitenciario de Argentina

Safe Network Model for M-Learning in prisons of the Argentine penitentiary system

Andrés Diaz[1], Fernando Lazo[1], Sergio Rocabado[2], Susana Herrera[1]

[1] Universidad Nacional de Santiago del Estero, Instituto de Investigación en Informática y Sistemas de Información, Santiago del Estero, Argentina

[2] Universidad Nacional de Salta, Departamento de Informática, Salta, Argentina

andy.sde@gmail.com, ferulazo@gmail.com, sergiorocabado@gmail.com, sherrera@unse.edu.ar

Recibido: 26/02/2021 | **Corregido:** 30/12/2021 | **Aceptado**: 24/02/2022

Cita sugerida: A. Diaz, F. Lazo, S. Rocabado and S Herrera, “Modelo de Red seguro para M-Learning en cárceles del sistema penitenciario de Argentina,” *Revista Iberoamericana de Tecnología en Educación y Educación en Tecnología*, no. 32, pp. 54-65, 2022. doi: 10.24215/18509959.32.e6

Resumen

Una persona privada de su libertad posee un escenario desalentador a causa de factores como la exclusión de la sociedad, el encierro y la falta de comunicación. La reinserción de estas personas en la sociedad constituye un gran desafío; y la educación es el medio principal por el cual se lo puede lograr. El M-Learning permite utilizar los dispositivos móviles para el proceso de aprendizaje. Sin embargo, es complicado utilizar dichos dispositivos en las penitenciarías, por razones de seguridad. En este artículo se propone un modelo de red MANET que permita el M-Learning en penitenciarías o cárceles. Se determinan cuáles son los componentes de la red y su configuración. La red fue diseñada en función de la información tomada de una penitenciaría de la provincia de Santiago del Estero, Argentina y fue validada en un entorno simulado que replica las condiciones del contexto. Los resultados fueron positivos; por lo tanto, la red propuesta está en condiciones de ser implementada en este tipo de ambientes, siguiendo ciertas recomendaciones específicas.

Palabras clave: Redes MANET; M-Learning; Seguridad en redes; Educación en penitenciarías.

Abstract

A person deprived of his or her liberty has a discouraging scenario because of factors such as exclusion from society, confinement and lack of communication. Reinserting these people into society is a great challenge; and education is the main means by which this can be achieved. M-Learning makes it possible to use mobile devices for the learning process. However, it is difficult to use such devices in prisons, for security reasons. This article proposes a model of a MANET network that allows M-Learning in penitentiaries or prisons. The components of the network and their configuration are determined. The network was designed based on information taken from a penitentiary of the province of Santiago del Estero, Argentina and it was validated in a simulated environment that replicates the conditions of the context. The results were positive; therefore, the proposed network is in a position to be implemented in this type of environment, following certain specific recommendations of the authors.

Keywords: MANET Networks; M-Learning; Network security; Education in prisons.

1. Introducción

La educación se fue constituyendo en una herramienta indispensable a la hora de re-insertar a una persona que ha estado en situación de encierro durante un tiempo prolongado, tal es así que se ha convertido en una actividad de mucha importancia dentro del sistema penitenciario [1]. El uso de la tecnología de comunicaciones en este ambiente generalmente no es permitido, al menos en Argentina, debido a la incapacidad de poder lograr un uso adecuado de la misma, siendo considerada una fuente principal de riesgo para el mantenimiento de la armonía en la prisión. Recién a partir de la aparición del Coronavirus, la justicia les permitió a los reclusos de la provincia de Buenos Aires, disponer de celulares para comunicarse con sus familias, pero sólo mientras dure el confinamiento ocasionado por la pandemia [2]. Sin embargo, se debe tener en cuenta que los sistemas tecnológicos y el aprendizaje mediado por dispositivos móviles (*M-Learning*) son elementos fundamentales en la actualidad, tal como quedó demostrado durante la pandemia de Coronavirus. Es importante sacar provecho de sus beneficios.

Los dispositivos móviles representan una gran alternativa para el aprendizaje en estos lugares debido a su fácil portabilidad y la capacidad que tienen para formar redes *Ad Hoc*, las cuales tienen la gran ventaja de no necesitar ninguna infraestructura fija, como se demostró en [3]. Y si se habla de dispositivos móviles y redes *Ad Hoc*, inevitablemente se debe nombrar a las MANET (*Mobile Ad-hoc Networks* – Red Móvil Ad-Hoc), las cuales son redes que combinan estos dos elementos.

Sin embargo, implementar una red de este tipo no es tan simple. Resulta necesario tener en cuenta qué dispositivos se deben emplear para que la red funcione correctamente, ya que cuentan con importantes limitaciones y desventajas, como ser:

- Cobertura limitada: dependiendo de la localización, la velocidad de transferencia puede disminuir drásticamente.
- Energía limitada: se debe tener en cuenta el consumo energético del mismo. Esto se agrava si se considera la imposibilidad de contar con enchufes conectados a la red eléctrica en los espacios donde se brindan las clases, por cuestiones de seguridad.
- Vulnerabilidad: debido a su fragilidad y escaso tamaño, los dispositivos corren el riesgo de ser extraviados, dañados o robados.

  Por otro lado, en las MANET es importante considerar los siguientes aspectos:

- No existe orientación a la conexión. Cada uno de los paquetes pueden seguir rutas distintas entre el origen y el destino, por lo que pueden llegar desordenados o duplicados. Sin embargo, el hecho de no ser orientado a conexión tiene la ventaja de que no se satura la red. Además, para elegir la ruta existen algoritmos que "escogen" qué ruta es mejor. Estos algoritmos se basan en la calidad del canal, en la velocidad del mismo y, en algunos, oportunidad hasta en 4 factores (todos ellos configurables) para que un paquete "escoja" una ruta.
- Seguridad: la seguridad es una parte muy importante en la implementación de una MANET. Al no poseer una infraestructura fija, y por ende carecer de un servidor de monitoreo centralizado, resulta más complicado supervisar el tráfico. Además, al poseer una topología dinámica, existen problemas para identificar y realizar un control de acceso de los dispositivos que ingresan y abandonan el sistema.

Tal como se muestra en este artículo, para implementar una MANET en una penitenciaria es necesario tener en cuenta las limitaciones presentadas. Pero, debido al contexto, es fundamental hacer hincapié en la seguridad. Como consecuencia de esto, es necesario que los nodos móviles sean especialmente configurados ya que, por cuestiones de seguridad, los mismos no deben tener acceso a la red de datos 3G ni a redes *WIFI. Bluetooth* se convierte en la alternativa ideal para configurar la red, gracias a su alcance limitado. Si bien existen otros protocolos que permiten reforzar la seguridad, estos afectan sensiblemente el uso de ancho de banda y el consumo de energía del dispositivo.

Teniendo en cuenta todo lo planteado, en este trabajo se propone un modelo de configuración de red que permite a reclusos de una penitenciaria, acceder a contenidos educativos desde sus dispositivos móviles (*M-Learning*), de forma segura y con la mayor eficiencia posible. El trabajo se desarrolló en la Unidad Penal de Varones Nº1 de la Provincia de Santiago del Estero.

Las principales etapas de la metodología que se empleó para diseñar y validar dicho modelo de red, se mencionan a continuación. El primer paso fue determinar qué necesidades educativas y de seguridad debían ser cubiertas para que el modelo sea factible. Para obtener las mismas, se realizaron entrevistas a personal de seguridad de la penitenciaria y a un docente que dicta clases en dicho establecimiento. Posteriormente, se analizó el contexto para determinar, tanto los recursos disponibles, como las limitaciones que se debían tener en cuenta a la hora de diseñar una red. Luego, se diseñó el modelo de red teniendo en cuenta los requisitos, las limitaciones y se establecieron las métricas a emplear para su validación. Posteriormente, se procedió a configurar todos los dispositivos participantes para ejecutar la validación, la cual arrojo una serie de resultados que posteriormente fueron calificados y analizados para determinar la factibilidad de implementar dicha configuración en el ambiente de trabajo.

A continuación, el presente artículo se organiza de la siguiente manera. En el apartado 2 se presentan los marcos referenciales que dan sustento al modelo diseñado. En el apartado 3 se detallan los requerimientos de seguridad y educativos, una descripción del ambiente de trabajo y concluye con el modelo de red. Posteriormente, en el apartado 4 se lleva a cabo la validación del modelo teniendo en cuenta diferentes parámetros. En el apartado 5

se presenta el análisis de los resultados obtenidos. Finalmente, en el apartado 6 se exhiben las conclusiones.

2. Marcos Referenciales

2.1. M-learning

M-Learning es un aprendizaje basado en dispositivos móviles, cuya fortaleza consiste en promover prácticas de aprendizaje en contextos propios del alumno, conectando los conocimientos teóricos con la vida cotidiana, proporcionando un aprendizaje situado, auténtico, sensible al contexto, personalizado, basado en juegos [4], [5], [6].

Las tecnologías móviles aplicadas a la educación promueven el desarrollo de competencias en forma autónoma, centrado en el aprendiz, lo cual constituye un requerimiento en diversos contextos educativos, por ejemplo, en las cárceles o penitenciarías.

El grupo de investigación de Computación Móvil de Universidad Nacional de Santiago del Estero (UNSE) ha venido estudiando diversas formas de implementar *M-Learning* en niveles educativos, contextos y áreas de aprendizaje diferentes.

Uno de los resultados más importantes de la investigación realizada por este grupo es haber elaborado MADE-mlearn, que constituye un marco sistémico y ecológico para el análisis, diseño y evaluación de experiencias de *M-Learning* [7]. Dicho marco fue utilizado para el diseño de actividades de *M-Learning* propuestas en este trabajo.

Sobre dicho marco el grupo implementó otras experiencias de *M-Learning* en Argentina [8], [9], [10].

2.2. Redes de computadoras

Según [5], una red es un conjunto de tecnologías (incluyendo *hardware, software* y medios) que se puede utilizar para interconectar computadoras, que les permite comunicarse, intercambiar información y compartir recursos en tiempo real.

Existen atributos de seguridad que toda red de computación, sin importar de qué tipo fuere, necesita cumplir para mantener el intercambio de información libre de riesgo y proteger los recursos informáticos de los usuarios y las organizaciones. Según [6], estos atributos son los siguientes:

- **Autenticación**: es básicamente la confirmación de que las partes intervinientes en una comunicación son quienes dicen ser y no son falsas. Esto requiere que los nodos, de alguna manera, demuestren que sus identidades son las que dicen ser. Sin autenticación un nodo podría hacerse pasar por un usuario (suplantación de identidad) y recibir información clasificada o sensible.
- **Confidencialidad**: asegura que un intruso no podrá ser capaz de acceder a información que se encuentra en tránsito entre dos nodos. Para esto emplea mecanismos de cifrado con el fin de evitar que nodos intermedios y no confiables comprendan el contenido de los paquetes transmitidos.
- **Integridad**: es la garantía de que el mensaje o paquete que está siendo entregado no ha sido modificado durante el tránsito o, de otra manera, que lo que ha sido recibido es exactamente lo que originalmente había sido enviado. Un mensaje se puede corromper por razones maliciosas y no maliciosas. El primer caso hace referencia a la modificación intencional de un mensaje por parte de un atacante. El segundo caso podría ocurrir producto de la debilitación de radio de propagación.
- **No repudio**: significa que el remitente de un mensaje no puede negar más adelante el envío de la información y que el receptor no puede negar la recepción. Esto es útil para detectar y aislar nodos comprometidos. Cualquier nodo que reciba un mensaje erróneo puede acusar al remitente con la prueba, informando así a los otros nodos sobre el nodo comprometido.

2.2.1. Redes Privadas Virtuales

Una Red Privada Virtual (VPN) es un grupo de computadoras interconectadas, ubicadas en distintas áreas geográficas, y que componen entre ellas una red privada denominada virtual porque no se conecta mediante un enlace físico, sino a través de una red pública como Internet. Una VPN protege la confidencialidad e integridad de los datos, garantizando que todo el tráfico que circule a través de la red, estará codificado y será de acceso sólo a los dispositivos autorizados.

Para entender el funcionamiento de una VPN, ésta se puede representar como una ruta con un inicio, un final y con diferentes puntos de control por donde viajan los paquetes de información. Al usar una VPN se aplica una capa de cifrado y autenticación para proteger el tráfico por donde viajan los datos. Esta técnica se llama *Tunneling* y crea un túnel o canal de comunicación dentro de una red de computadoras. De esta manera, los nodos intermedios que participen en la comunicación van a interactuar con el paquete, pero solamente al final de la comunicación la información podrá ser descubierta y descifrada para su uso. La capa de autenticación va a verificar la identidad de los usuarios y a restringir el acceso a quienes no estén autorizados [7]. En la Figura 1, se muestra un paquete cifrado característico del protocolo *OpenVPN* (Protocolo de código abierto empleado para realizar conexiones punto a punto seguras) viajando por el túnel privado.

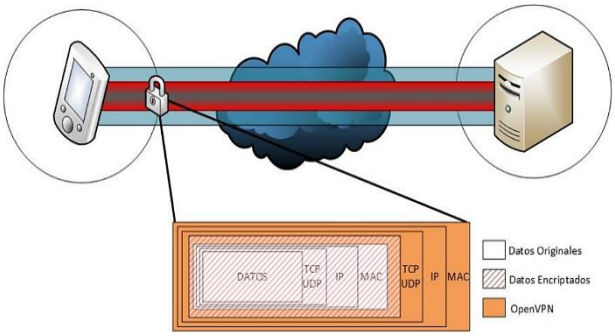

Figura 1. Túnel OpenVPN

2.2.2. Redes Inalámbricas

Las redes inalámbricas son redes en las que dos o más nodos (por ejemplo, *notebook, netbook, smartphone*, etc.) se comunican sin la necesidad de una conexión por cable. Esto permite que un usuario pueda mantenerse conectado mientras se desplaza cómodamente dentro de una determinada área geográfica. Las redes inalámbricas se basan en un enlace de ondas electromagnéticas, ya sean radio o infrarrojo, en lugar de cableado estándar. Hay variedad de tecnologías inalámbricas, las cuales se diferencian por la frecuencia de transmisión, el alcance y la velocidad de transmisión [8].

Las redes inalámbricas presentan una serie de ventajas que las hace ideales para usar en un ambiente de *M-Learning* dentro de una penitenciaria. No existen cables físicos que entorpezcan la movilidad permitiendo, además, que se puedan desplegar en áreas complicadas o remotas, incluso con gran cantidad de dispositivos móviles conectados.

Sin embargo, también poseen desventajas que deben ser tenidas en cuenta. Por su naturaleza inalámbrica, son un poco más inestables que las redes cableadas ya que pueden verse afectadas por otras ondas electromagnéticas o, incluso, por objetos tales como paredes, espejos, etc. Su ancho de banda es menor que las redes cableadas y, por último, son más inseguras porque los paquetes no viajan por un medio físico sino a través del aire [9].

2.2.3. MANET

Según [10], una red móvil ad hoc o MANET es una colección de nodos inalámbricos móviles que se comunican de manera espontánea y auto-organizada constituyendo una red temporal sin la ayuda de ninguna infraestructura preestablecida (como puntos de acceso *WiFi* o torres de estaciones base celulares con antenas 2G o 3G) ni administración centralizada. Las estaciones inalámbricas, además de ofrecer funcionalidades de estación final, deben proporcionar también servicios de enrutamiento, retransmitiendo paquetes entre aquellas estaciones que no tienen conexión inalámbrica directa. Las redes *ad hoc* pueden desplegarse de forma completamente autónoma o combinarse con las redes locales inalámbricas para conectarse a internet utilizando puntos de acceso inalámbricos. Este tipo de redes puede adaptarse dinámicamente ante los cambios continuos de las características de la red, tales como la posición de las estaciones, la potencia de la señal, el tráfico de la red y la distribución de carga, siendo el reto principal los continuos e impredecibles cambios en la topología de la red.

2.2.4. Especificación 802.15.1: Bluetooth

Bluetooth es una tecnología *Wireless ad hoc*, de bajo costo y poca potencia que permite implementar una MANET, aunque no incorpora los protocolos de enrutamiento de la misma. Esta tecnología se encuentra especificada en el estándar 802.15.1 de la IEEE [11].

La unidad básica de un sistema *Bluetooth* es una *piconet*, que consta de un nodo maestro y hasta siete nodos esclavos activos a una distancia de 10 metros. En una misma sala (grande) pueden encontrarse varias *piconets* y se pueden conectar mediante un nodo puente como lo muestra la Figura 2. Un conjunto de *piconets* interconectadas se denomina *scatternet* [6].

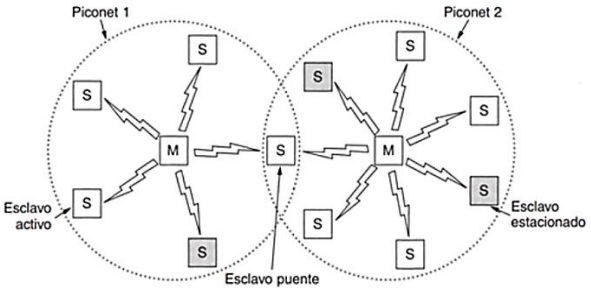

Figura 2. Piconets Interconectadas formando una Scatternet

Además de los siete nodos esclavos activos de una *piconet*, puede haber hasta 255 nodos estacionados (*parked*) en la red. Éstos son dispositivos que el nodo maestro ha cambiado a un estado de bajo consumo de energía para reducir el desgaste innecesario de sus pilas. Lo único que un dispositivo en este estado puede hacer es responder a una señal de activación por parte del maestro.

Bluetooth ofrece autenticación, autorización y encriptación a nivel de enlace [12]. Para mantener la seguridad en la capa de enlace, se usan 4 componentes diferentes:

- *Bluetooth Device Address* (BD_ADDR) de 48 bits
- Una clave de usuario privada de 128 bits para la autenticación
- Una clave de usuario privada para encriptación de tamaño variable entre los 8 y los 128 bits
- Un número aleatorio generado para cada nueva conexión de 128 bits

Las claves secretas se generan durante el inicio de la conexión. Primero se genera la clave de autenticación y a partir de esta, se genera la clave de encriptación, sin embargo, ambas son diferentes. Cada vez que se activa la encriptación, se genera una nueva clave. Uno de los parámetros que se utiliza para generar la clave de

autenticación es el PIN (numero decimal de 4 dígitos), el cual en los casos en el que sea posible, es ingresado por el usuario. A partir de las diferentes especificaciones de *Bluetooth* se fueron definiendo modos de seguridad. Como se puede observar en la tabla 3, existen en total tres modos de seguridad en *Bluetooth* según describe [12] y cada dispositivo debe operar con sólo uno a la vez. Ellos son los siguientes:

- Modo de seguridad 1: No posee ningún tipo de seguridad, autenticación ni encriptación. Las conexiones quedan susceptibles a atacantes. Soportado por las versiones 2.0 y anteriores.
- Modo de seguridad 2: Seguridad obligatoria a nivel de servicio. Permite controlar el acceso a determinados servicios y dispositivos. Permite definir diferentes políticas de seguridad y niveles de confianza para cada petición.
- Modo de seguridad 3: seguridad a nivel de enlace. Todas las conexiones entre dispositivos deben estar autenticadas y encriptadas.

Bluetooth dispone además de un perfil denominado *Personal Area Networking* (PAN), tal como se describe en [13], que proporciona el transporte de datagramas IPv4 mediante el protocolo *Bluetooth Network Encapsulation Protocol* (BNEP) que provee capacidades similares a Ethernet y posee un formato de encapsulamiento que hace un uso eficiente del ancho de banda [14].

3. Modelo de Red

3.1. Necesidades planteadas por el cuerpo docente

Para determinar las necesidades educativas existentes en el ámbito penitenciario, se realizó una entrevista al personal docente de la Unidad Penal de Varones Nº 1 de Santiago del Estero. Las mismas arrojaron los siguientes resultados:

- Es necesario considerar que la incorporación de tecnología móvil debe ser lo más sencilla y adaptable posible, sobre todo si se tiene en cuenta a las personas de mayor edad, las cuales pueden poseer mayor dificultad que otras en el aprendizaje y uso de los dispositivos móviles
- La inserción de dispositivos móviles tiene como objetivo colaborar en el proceso de aprendizaje. Sin embargo, muchas personas se pueden distraer con los mismos, desviando su atención en la clase y como consecuencia impidiendo que se cumpla con el propósito original del proyecto. Para evitar esto, es necesario implementar permisos adecuados para el uso de aplicaciones
- Una de las razones por las que la tecnología fue tan resistida dentro de las penitenciarías, fue por la dificultad de implementar las medidas de seguridad adecuadas para dicho entorno. Por este motivo, es sumamente importante la implementación de mecanismos de seguridad que garanticen un uso adecuado de los dispositivos, y establezcan un entorno seguro de trabajo
- El cuerpo docente planteó la necesidad de disponer de bibliografía en formato electrónico, emplear recursos visuales, tales como gráficos, tablas y herramientas que permitan generar una interacción entre el docente y los alumnos para aclarar dudas y compartir opiniones. Por ello es necesario que la propuesta disponga de una plataforma educativa capaz de ofrecer estos recursos.

3.2. Necesidades de seguridad impuestas por el sistema penitenciario

A través de entrevistas y charlas realizadas a las autoridades del penal, se pudieron establecer las siguientes pautas mínimas de seguridad que debería satisfacer la red diseñada:

- Garantizar la privacidad de los datos que un usuario esté enviando, impidiendo que alguien los intercepte y pueda leerlos o emplearlos con fines indebidos, así como imposibilitando la identificación del emisor original
- Negar el acceso a personas no autorizadas a la información compartida por quienes participan en la clase. Para ello se implementó un sistema de contraseñas
- Asegurarse que los datos recibidos por las personas que participan en clase no sean modificados, con el objetivo de evitar que los mismos puedan llegar a contener alguna información indebida, que incite a llevar a cabo alguna acción ilícita a un interno
- Impedir el acceso libre a Internet, permitiendo sólo la utilización de este servicio para obtener los documentos necesarios para la clase
- Denegar el acceso a aplicaciones que no contribuyan al proceso de aprendizaje, con el fin de evitar distracciones durante la sesión educativa.
- Impedir que los dispositivos (a excepción del usado por el docente) puedan comunicarse por redes celulares.

3.3. Descripción del Ambiente

En cuanto a la infraestructura edilicia, el Penal posee aulas destinadas a la educación de los internos ubicadas en su último piso (2do). Las paredes que componen la estructura son de ladrillo y poseen un grosor de 30 cm. El ladrillo provoca una atenuación media a la señal inalámbrica [15]. En las aulas no se encuentran tomacorrientes, como medida preventiva de seguridad.

3.3.1. Señales Inalámbricas

Se realizó una medición con un celular abonado a la empresa de telefonía *Claro*, empleando la aplicación *Network Cell Info Lite* en su versión 3.40 [16]. Se pudo comprobar que en el lugar se recibe señal 4G LTE (*Long Term Evolution*). La Potencia de recepción de señal RSRP fue -88 dBm, que corresponde a una señal media-alta. La relación señal-ruido (*signal to noise ratio* -SNR) se encuentra en 8.0 dB lo que significa que existen fuentes de ruido en el lugar, pero que no representan una degradación importante en el funcionamiento de la red celular (ver Figura 3). Este ruido es generado por otros dispositivos que generan transmisiones en la misma banda de frecuencias.

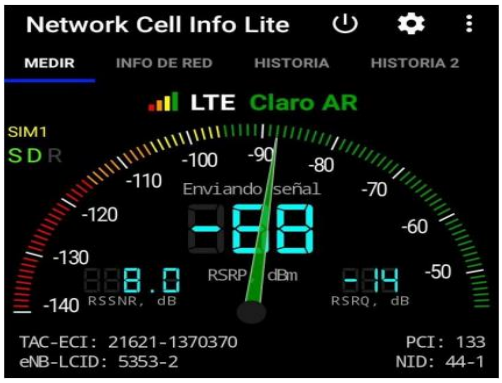

Figura 3. Resultado de prueba de intensidad de señal

Las velocidades de descarga promedio fueron medidas con la herramienta *Speedtest*, versión 3.2.32 [17]. La velocidad media de descarga ronda los 4,47 MB/s, obteniendo como valor inferior unos 2,40 MB/s de descarga y como valor superior unos 6.54 MB/s. En cuanto a la velocidad de carga, la misma se ubicó aproximadamente en 7,53 MB/s, obteniendo como valor inferior una velocidad de 2.59 MB/s y como valor superior unos 12.47 MB/s. Se debe tener en cuenta que estas mediciones se hicieron desde un dispositivo conectado directamente a la red de datos de la compañía Claro.

Posteriormente, se realizó una prueba de ancho de banda desde un dispositivo esclavo conectado al *Gateway* por anclaje *Bluetooth* para obtener acceso a Internet. Los resultados fueron en promedio una descarga de 0,72 Mbps y una carga de 0,64 Mpbs. Esta diferencia en las velocidades se da por una limitación estándar de *Bluetooth* PAN que, según [18], admite como máximo una tasa de transferencia de 1Mbps en un rango de 10 metros.

3.4. Modelo de red propuesto

El modelo de red propuesto (ver Figura 4) consta de una MANET, implementada dentro de la penitenciaria, conformada por dispositivos móviles con dos tipos de funciones específicas. Uno de ellos, denominado "nodo maestro" actúa como *Gateway* o puerta de enlace a la red de datos móviles, el cual tiene como función principal, compartir internet hacia los demás dispositivos móviles, denominados "nodos esclavos", mediante anclaje *Bluetooth*. De esta manera, cada uno de estos nodos puede acceder al servidor *M-Learning* a través de una conexión segura (VPN). En el modelo propuesto se realizan túneles privados entre cada uno de los dispositivos móviles y el router *MikroTik*. De esta forma se garantiza que los únicos dispositivos que se pueden conectar a la red de infraestructura son los autorizados. La autorización de los mismos se realiza mediante el uso de certificados individuales para cada cliente.

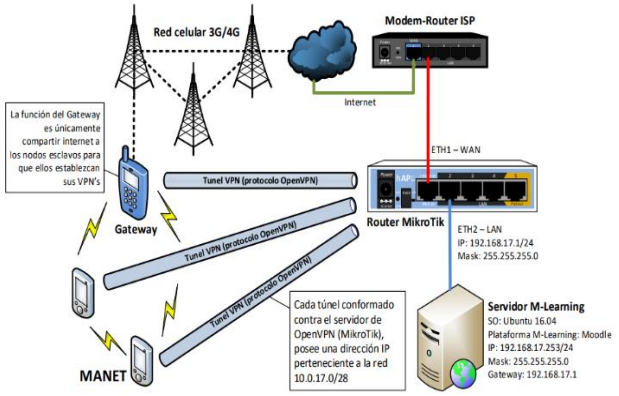

Figura 4. Conexión entre MANET y red de infraestructura

3.4.1. Red de infraestructura del servidor M-Learning

La red en donde se ubica el servidor *M-Learning*, está conformada mínimamente por tres dispositivos, el servidor y dos *routers*; los cuales están interconectados mediante cable de par trenzado UTP con protocolo *Ethernet* (Figura 5). Un *router* es el encargado de proveer Internet para realizar la interconexión con la MANET por medio de una VPN. Dicho *router* debe ser provisto por el ISP (proveedor de servicio de Internet) contratado y sus configuraciones deben ser las incluidas por defecto. El servicio de Internet puede estar encaminado vía cable telefónico, fibra o coaxial indistintamente. El otro *router* cumple una función importante dentro de este diseño ya que es el encargado de implementar la seguridad necesaria para proteger al servidor y de conformar la VPN. Por ello es necesario que el mismo sea administrable y que posea estas funcionalidades. Por su estabilidad, confiabilidad, funcionalidad se hizo uso de un *Router MikroTik*, el cual funciona con el sistema operativo *RouterOS*.

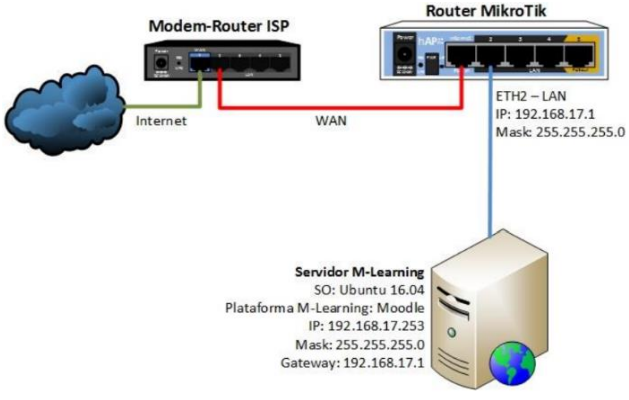

Figura 5. Red de Infraestructura

El servidor *M-Learning* funciona bajo el sistema operativo Ubuntu, tiene instalado un *software* LMS (*Learning Management System*) que gestiona los contenidos educativos. Para esta propuesta, se emplea la plataforma *Moodle* como LMS. Para que esta funcione debidamente, es necesario que el servidor actúe como web Server por lo que se emplea el servidor web Apache que implementa el protocolo HTTP. Para la administración de los datos, Moodle emplea MySQL. Además, es necesario instalar PHP 7.0 para que el servidor pueda ejecutar las sentencias desarrolladas en este lenguaje.

3.4.2. Conexión de la MANET con la red de Infraestructura

Para integrar la MANET, ubicada en la Unidad Penal de Santiago del Estero, con la red de infraestructura donde se encuentra el servidor *M-Learning*, se optó por generar túneles privados individuales entre cada dispositivo móvil y el *router MikroTik* a través de la red de datos móviles, empleando la tecnología 3G/4G. Esta elección se fundamenta en las siguientes razones:

- Las unidades penitenciarias generalmente no se encuentran en zonas demasiado alejadas del centro urbanístico, por lo que disponen de tecnologías 3G y hasta 4G
- Las altas velocidades máximas de transferencia soportadas por las redes 3G y 4G permiten implementar conexiones extremadamente seguras con la red de infraestructura, sin disminuir su desempeño
- Los dispositivos actuales disponen mínimamente de tecnología 3G
- Esta tecnología tiene alcance en gran parte del territorio argentino y podría ser empleada en zonas remotas, carentes de proveedores de servicio de internet.

3.4.3. Red dentro del sistema penitenciario (MANET)

Para conformar la red MANET se recomienda como mínimo el uso de dispositivos móviles, ya sean *Tablet* o *Smartphones* que cuenten con las siguientes características:

- Red móvil 3G o 4G
- Bluetooth 4.0 o superior
- Sistema operativo Android 4.1.2 o superior. Se decidió usar dispositivos con este sistema operativo ya que, permiten una mayor amplitud de configuración vía consola y menú de opciones para desarrolladores.
- 2 GB de RAM o más
- 8GB de memoria interna o mas

Para desplegar la MANET se eligió la tecnología *Bluetooth* (IEEE 802.15.1) por las siguientes razones:

- Utiliza un radio de corto alcance que ha sido optimizado para el ahorro de energía
- Su bajo precio y reducido tamaño, posibilitan que la mayor parte de los dispositivos móviles que se consiguen en el mercado tengan incorporada la interfaz Bluetooth
- Facilidad y rapidez de despliegue. Bluetooth no utiliza componentes de infraestructura
- Posibilidad de usar el perfil PAN, como se mencionó anteriormente, para el transporte de datagramas IPV4 mediante el protocolo BNEP
- En el escenario propuesto, la conexión del dispositivo móvil cliente al punto de acceso a la red (*NAP - Network Access Point*) se realizó utilizando el perfil PAN (*Personal Área Network*) del estándar *Bluetooth*. El punto de acceso a la red se configuró sobre el nodo *Gateway* utilizando la funcionalidad *Bluetooth Tethering* de *Android*, que utiliza el Framework *netfilter* e *iptables* para implementar un puente entre la PAN Bluetooth y la red celular.
- Seguridad: como característica fundamental para la elección de esta tecnología, se encuentra la imposibilidad de usar redes *WiFi* o redes celulares por cuestiones de seguridad
- *Bluetooth* cuenta con un ancho de banda de 24 Mbps en su versión 3 y de hasta 32 Mbps en su versión 4 respectivamente [11], estos valores constituyen un sustento aceptable para avalar el trabajo que se desea realizar.

En la penitenciaria se implementa una MANET integrada por dos tipos de dispositivos móviles, uno que actúa como *gateway* o puerta de enlace, a cargo del docente de cátedra y los nodos que cumplen la función de esclavos, utilizados por los estudiantes (Figura 6).

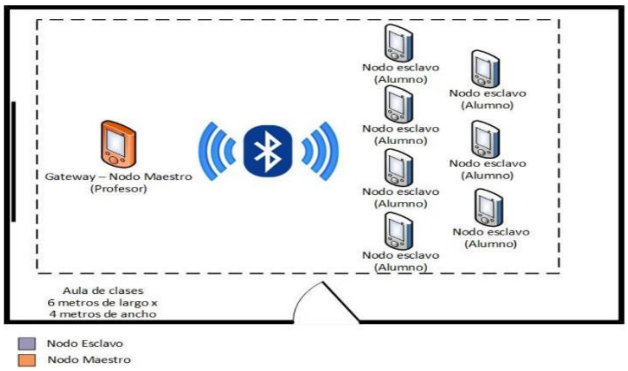

Figura 6. Diseño detallado de la MANET

Los dispositivos que conforman esta red se limitaron a una cantidad total de ocho (7 esclavos y un nodo maestro). Esta limitación existe debido a la estructura que compone a una *piconet*, la cual restringe la cantidad de nodos interconectados. Pese a poder expandir la cantidad de nodos participantes a través de la unión de varias *piconets*, formando una *Scatternet* (Figura 2), esto no fue considerado, ya que la cantidad promedio de estudiantes

por clase es de seis alumnos más el profesor en el caso del estudio abordado.

En el modelo propuesto, los dispositivos esclavos no tienen conexión a la red inalámbrica celular (3G o 4G). Únicamente el nodo *gateway* o maestro (usado por el docente) tiene acceso a la red móvil celular para poder compartir vía *Bluetooth* la conexión a internet a los demás dispositivos de manera controlada de forma que puedan recuperar los contenidos ubicados en el servidor *M-Learning*, a través de una VPN. El dispositivo *gateway* también posee un certificado que le permite establecer un túnel y acceder a los contenidos educativos, ya que es necesaria la participación activa del profesor.

3.4.4. Seguridad

Teniendo en cuenta los atributos de seguridad necesarios que debe satisfacer una red, los cuales fueron abordados en el apartado 2, se detallan a continuación los niveles de seguridad implementados en la red propuesta: nivel de aplicación, nivel de red y nivel físico.

La seguridad a nivel de aplicación esta implementada en la plataforma Moodle, a través de la Autenticación de Usuarios, cada uno de los cuales tiene uno de los tres niveles de privilegios siguientes: gestor, profesor, estudiante.

Con el objetivo de impedir la navegación y el acceso a configuraciones sensibles del usuario, se emplean dos aplicaciones:

/*system/app* mover [19]: convierte las aplicaciones que el administrador indique, en aplicaciones de sistema, evitando de esta manera, que las mismas puedan eliminarse.

Privacy Protector [20]: bloquea el acceso libre a las aplicaciones sensibles del teléfono. Es importante destacar que este programa no trabaja como *firewall*, por lo que no bloquea el funcionamiento de las aplicaciones, sólo impide al usuario el acceso a algunas de ellas, previamente definidas por el administrador y protegidas por contraseña.

Además, empleando el gestor de archivos ES *File Explorer* [21] para ingresar y modificar archivos de sistema, se deshabilita el servicio de *WiFi* de cada teléfono empleado por los alumnos.

A nivel de Red, la seguridad está dada por el uso de una VPN basada en el protocolo *OpenVPN*, la cual conforma un enlace seguro extremo a extremo entre cada nodo perteneciente a la MANET y el *router MikroTik* perteneciente a la red de infraestructura, aislando a cada uno y evitando la necesidad de agregar sobrecarga a la red implementando HTTPS. Se escogió este protocolo por las siguientes razones:

- Se puede configurar para que corra en cualquier puerto, lo que hace que sea extremadamente difícil de bloquear por medio de cortafuegos
- El sistema de criptografía se basa en *OpenSSL*
- Soporta una variedad de algoritmos criptográficos, tales como 3DES, AES, *Camellia*, *Blowfish*, CAST-128
- Es una aplicación de libre distribución (licencia open source)
- Es multiplataforma, se ejecuta sobre Android y iOS.

Además, el router *MikroTik* debe tener implementado un conjunto de reglas de *firewall* para brindar una primera defensa a la red de infraestructura y prevenir ataques de denegación de servicios lógicos contra la red.

Es necesario garantizar que no cualquier dispositivo pueda conectarse a la red de infraestructura LAN, a excepción de aquellos que estén autorizados a hacerlo.

Además, se restringe el acceso a servicios no necesarios desde la MANET, mediante el filtrado de puertos. Para ello, se definen reglas de filtrado que realizan las siguientes acciones:

- Denegar conexiones inválidas: bloquea paquetes TCP con combinaciones de *flags* inválidas
- Permitir tráfico proveniente desde la VPN
- Permitir tráfico proveniente desde la red LAN
- Permitir el acceso al *router MikroTik* únicamente desde el servidor *M-Learning*
- Permitir conexiones sólo a los puertos HTTP y HTTPS
- Permitir conexiones al puerto definido para *OpenVPN*
- Denegar todo lo demás.

En cuanto a la seguridad a nivel físico, para evitar el acceso a la red de datos celular, se recomienda el uso de dispositivos que no admitan chip de datos, por ejemplo, tabletas. En caso de emplearse *smartphones*, se aconseja que se remuevan las tarjetas SIM, salvo la del dispositivo que actúa como puerta de enlace.

Además, para ofrecer una alta disponibilidad, es necesario que el servidor este físicamente resguardado, en una habitación con acceso únicamente a personas autorizadas, ambiente acondicionado para evitar daños por recalentamiento de componentes, UPS para que posibles bajas o cortes eléctricos no afecten el normal funcionamiento del servidor o pongan en riesgo la integridad del mismo y el uso de redundancia en los discos (RAID) para evitar la pérdida de datos en caso de roturas en las unidades de almacenamiento permanente.

4. Validación del modelo propuesto

Por razones de seguridad, fue imposible realizar la simulación en el ambiente real, por lo que se llevó a cabo la validación en un entorno con características similares.

El testeo se llevó a cabo en una de clase de 30 minutos, en la cual se verificó el funcionamiento del modelo propuesto. Se emplearon 6 *smartphones*, 5 de los cuales se

encontraban vinculados al nodo *gateway* mediante *Bluetooth*. El nodo maestro fue el único con acceso a la red de datos 4G. Durante el transcurso de esta validación, se accedió al servidor *M-Learning* mediante el uso de la plataforma Moodle. En dicha plataforma se creó un curso denominado Informática en el cual estaban implementados foros de discusión y otras actividades que involucraban el acceso a documentos en línea, observar imágenes, leer texto, etc. Se realizaron mediciones para validar el funcionamiento del modelo propuesto, teniendo en cuenta distintas métricas, como el desempeño de las conexiones *Bluetooth* en diferentes distancias, el tiempo de ida y vuelta de una solicitud, la tasa de transferencia efectiva (*Throughput*) y el consumo de batería.

4.1. Tiempo de ida y vuelta (RTT)

Para verificar la efectividad de la conexión *Bluetooth* que vincula los dispositivos que conforman la MANET, se realizaron pruebas de conexión mediante el envío de paquetes ICMP al servidor Moodle.

Los resultados arrojados se expresan en la Tabla 1 y muestran un RTT (*Round Trip Time o* tiempo de ida y vuelta) promedio de 280 milisegundos con el 100% de paquetes recibidos. Teniendo en cuenta las recomendaciones de la *International Communications Union* (ITU) [22] acerca de la latencia en un sentido, la cual no debe superar los 400ms, queda demostrado que el funcionamiento de la MANET será óptimo dentro de distancias iguales o inferiores a 10 metros.

Tabla 1. Pruebas de conexión Bluetooth sobre 10m

Distancia	Longitud de paquete	Paquetes enviados	Paquetes recibidos	Paquetes perdidos	TTL	RTT (ms)
10 Metros	10 bytes	10	10	0	64	276
10 Metros	25 bytes	10	10	0	64	292
10 Metros	50 bytes	10	10	0	64	260
10 Metros	100 bytes	10	10	0	64	303
10 Metros	200 bytes	10	10	0	64	271
Promedio RTT						**280**

4.2. Throughput

El *Throughput* es la cantidad de datos que realmente viaja a través del canal con éxito y permite dar una idea clara acerca de su rendimiento.

El experimento consistió en la descarga de un archivo de 6,96 MB, ubicado en el servidor *M-Learning*, desde un dispositivo móvil considerando diferentes tipos de conexiones y de VPN. Se repitió el proceso bajo las siguientes características para observar la diferencia en el comportamiento entre todas ellas.

- Empleando la conexión *Bluetooth* y 4G tal como se realizaría desde un nodo esclavo perteneciente a la MANET propuesta en el modelo.
- A través del enlace VPN de protocolo *OpenVPN* con 4G
- A través de la VPN de protocolo *OpenVPN* con *WiFi.*
- A través de una VPN PPTP no segura

En la Figura 7 se puede observar el tiempo que le demandó a cada tipo de conexión descargar el archivo. Vale destacar que la red de infraestructura se encuentra conectada a Internet a través de una conexión asimétrica, de 6MB de bajada y 1 MB de subida.

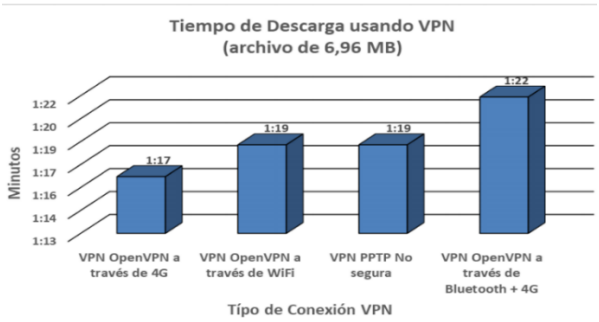

Figura 7. Grafico comparativo tiempos de descarga

En la Figura 8 se puede observar el *throughput* ofrecido para cada tipo de conexión. En él, se puede apreciar que el mejor rendimiento se obtiene al realizar la descarga a través del canal seguro *OpenVPN* y empleando directamente la conexión de 82 datos 4G. La conexión segura *OpenVPN* desde un nodo esclavo, empleando el internet compartido desde el nodo *Gateway* de la MANET vía *Bluetooth* y posteriormente a través de la red de datos, obtuvo aproximadamente un rendimiento inferior de 6%. Esto se explica por la sobrecarga de cabeceras empleadas para establecer la conexión (*overhead*).

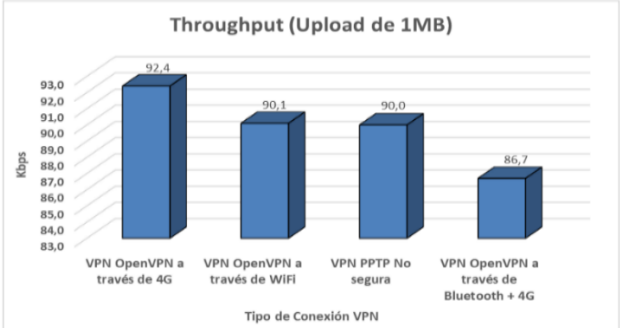

Figura 8. Grafico comparativo de eficiencia de la red

Para verificar el comportamiento de la red bajo esfuerzo, se realizó la descarga de un archivo PDF de 6,96 MB en forma simultánea desde los teléfonos de 5 usuarios, y se midió el *Throughput* y el tiempo de descarga para cada uno de ellos. Para realizar esta prueba se modificó el archivo php.ini de Moodle ya que, por defecto Moodle posee la limitación de subida de un archivo como máximo de 2MB.

En la tabla 2 se pueden observar los resultados.

*Tabla 2. R*esultados de descarga simultánea

Tamaño de Archivo	Cliente	Throuhgput (kbps)	Tiempo de descarga (segundos)
6,96 MB	Usuario 1	64,5	110
	Usuario 2	48,5	130
	Usuario 3	36,7	194
	Usuario 4	31,5	240
	Usuario 5	26,1	273

4.3. Consumo de Batería

En la Tabla 3, se puede observar que, en media hora de uso, los dispositivos consumieron en promedio sólo el 5% del total de la batería (la batería es de 2070 mAh). El mayor consumo de batería está dado por tener la pantalla activada, la cual equivale a un 74% del uso total mencionado. El *Bluetooth*, como se esperaba tuvo muy bajo consumo, sólo de 0.5% del total. Por otro lado, el *software* en su conjunto empleo el 25.5% de la batería consumida, correspondiendo la mayor parte de este consumo a servicios del sistema. El cliente *OpenVPN* sólo consumió un 0.7% del total y el navegador empleado (*Chrome*), un 7%.

Tabla 3. Consumo de batería

Tipo	Detalle	Consumo de batería	Totales
Hardware	Pantalla	74%	74,5% (3,73% del uso total de la batería)
	Bluetooth	0.5%	
Software	OpenVPN	0.7%	25,5% (1,27% del uso total de la batería)
	Google Chrome	7.0%	
	Sistema	13,3%	
	Otros Servicios	4.5%	
Uso total de Batería			5%
Temperatura de Batería			31º
Tiempo de simulación			30 min

5. Análisis de resultados

A partir de la validación realizada, es importante destacar las siguientes observaciones y recomendaciones.

1) La aplicación cliente *OpenVPN* no hace un empleo excesivo de los recursos del dispositivo móvil, ya que no requiere un uso intensivo ni del CPU ni de la batería. La cantidad de datos recibidos y enviados por la misma dependerá de los contenidos a los cuales se accedan.

2) Cuando los dispositivos se encuentran descargando un archivo de tamaño considerable de manera simultánea, los valores del *throughput* generados por los mismos van en descenso según la cantidad de dispositivos que estén realizando dicha tarea simultáneamente. Esto produce como consecuencia mayores tiempos de descarga. Los tiempos de descarga obtenidos, si bien varían desde los 110 a los 273 segundos, no representan un problema considerable.

3) Como consecuencia del punto anterior, no se recomienda el uso de recursos videográficos, ya que la reproducción de los mismos provocará saturación en la red, volviéndola lenta y dificultando su uso.

4) En cuanto al consumo de batería, el mayor uso está dado por la pantalla del dispositivo, a la cual le corresponde un 74% del total consumido durante la simulación. Al software le corresponde un 25,5% del consumo total de batería durante la simulación, el cual está dado mayormente por aplicaciones de sistema. Cabe destacar que elementos característicos de la propuesta presentada tales como el Bluetooth y el cliente *OpenVPN*, representan consumos mínimos de batería.

5) Si bien durante la simulación se pudo corroborar el funcionamiento fluido de la propuesta, no se puede asegurar esto en el total de los casos ya que se depende de factores externos como el estado de la conexión de datos móviles. Entre los casos que pueden generar ineficiencia en la red, se pueden citar el congestionamiento por la cantidad de usuarios empleando la red de datos móviles y posibles caídas del servicio de telefonía móvil.

6) Luego de probar varios dispositivos, de diferentes marcas y modelos, como puerta de enlace, se pudo notar que algunos permiten compartir internet vía *Bluetooth* a más nodos esclavos que otros. En caso de poseer un número de alumnos mayor al soportado, ya sea por el Gateway o por la tecnología Bluetooth para conformar la *piconet*, se sugiere el uso de dos o más *piconets* dependiendo de la cantidad de alumnos requerida.

7) En [23], se puede ver en detalle las configuraciones realizadas en el servidor (Instalación y configuración de plataforma *M-Learning*), en los dispositivos inalámbricos y en los dispositivos de red.

Conclusiones

En este artículo se ha presentado un modelo de red basado en tecnologías móviles que permite implementar *M-Learning* en penitenciarías de modo seguro. Dicho modelo fue descrito en el apartado 3 y fue validado en el apartado 4, obteniendo resultados que se consideran aceptables desde el punto de vista de la seguridad, el consumo de recursos y la fluidez con la que se desempeña la red.

A continuación, se presentan algunos trabajos futuros que pueden desarrollarse como resultado de esta investigación. Además, se sugieren algunos desarrollos específicos para apoyar y mejorar el modelo y metodología propuestos.

Entre los posibles trabajos futuros se destacan:

- Realizar el estudio para una cantidad mayor de alumnos, que plantee la necesidad de implementar una o más piconets para corroborar el desempeño del modelo bajo esas condiciones.
- Implementar el modelo dentro de una penitenciaria, lo que permitirá comprobar la eficacia del mismo en un ambiente real.
- Reemplazar la implementación de una MANET por la implementación de una Red Mesh, la cual es una

nueva característica que ofrece Bluetooth LE (*Low Energy*) y que no presenta la limitación en cantidad de nodos conectados simultáneamente como lo hacen las piconets.

Referencias

[1] M. Bengoa, S. Bruera and S. Lijtenstein, “Educación para la población privada de libertad: Diagnóstico y propuesta estratégica 2015-2025,” Informe de Consultoría, Proyecto OPP-Unión Europea, OIT/Cinterfor, 2015. [Online]. Available: https://www.oitcinterfor.org/sites/default/files/OIT_4_1_1_0.pdf

[2] Infobae, “Celulares en las cárceles: los presos tendrán permitido comunicarse por WhatsApp pero no podrán usar las redes sociales,” 2020. Recuperado de https://www.infobae.com/coronavirus/2020/03/31/celulares-en-las-carceles-bonaerenses-los-presos-tendran-permitido-comunicarse-por-whatsapp-pero-no-podran-usar-las-redes-sociales/

[3] S. H. Rocabado, “Caso de estudio de Comunicaciones Seguras sobre Redes Móviles Ad Hoc,” Tesis de MAestrìa en Redes de Datos, Facultad de Informática, Universidad Nacional de La Plata, 2013.

[4] J. Seipold and N. Pachler, “Evaluating Mobile Learning Practice Towards a framework for analysis of user-generated contexts with reference to the socio-cultural ecology of mobile learning,” *MedienPädagogik. Zeitschrift für Theorie und Praxis der Medienbildung*, vol. 19, 2011. [Online]. Available: https://www.researchgate.net/publication/233980956_Evaluating_mobile_learning_practice_Towards_a_framework_for_analysis_of_user-generated_contexts_with_reference_to_the_socio-cultural_ecology_of_mobile_learning

[5] M. Sharples, J. Taylor and G. Vavoula, “Theory of learning for the mobile age,” in *The Sage Handbook of E-learning Research*. C. Haythornthwaite, R. Andrews, J. Fransman and E. M. Meyers, Eds., London: Sage publications, 2007.

[6] N. Pachler, B. Bachmair and J. Cook, *Mobile learning: structures, agency, practices*. Nueva York: Springer, 2010.

[7] S. Herrera, C. Sanz and C. Fennema, “MADE-mlearn: un marco para el análisis, diseño y evaluación de experiencias de *M-Learning* en el nivel de postgrado,” *Revista Iberoamericana de Tecnología en Educación y Educación en Tecnología*, no. 10, 2013.

[8] S. Herrera and C. Sanz, “Collaborative *M-Learning* practice using Educ-Mobile,” in *International Conference on Collaboration Technologies and Systems (CTS)*, Minneapolis, USA: IEEE, 2014, pp. 363-370.

[9] S. Herrera, R. Palavecino, C. Sanz and J. Carranza, “Aprendizaje de Estructuras de Datos mediante *M-Learning*,” in *I Simpósio Ibero-Americano de Tecnologias Educacionais*, Araranguá, SC, Brazil, 2017.

[10] M. Morales, S. Herrera, M. Maldonado, P. Budán and F. Rosenzvaig, “M-Learning con Realidad Aumentada para el aprendizaje significativo en Álgebra Lineal,” *Revista Tecnologias na Educação*, vol. 24, 2018.

[11] P. Norton, *Introduccion a la Computación*. Mc Graw Hill, Sexta Edicion.

[12] A. S. Tanenbaum, *Redes de computadoras*. Pearson Educación, 2003.

[13] C. A. Calahorrano Vega, “Evaluación de rendimiento entre las tecnologias de EVPN y VPLS sobre una red MPLS en un ambiente Juniper simulado en GNS3,” Bachelor Thesis Universidad de las Fuerzas Armadas, 2019. [Online]. Available: http://repositorio.espe.edu.ec/handle/21000/15886

[14] C. Viloria Núñez, J. Cardona Peña and C. Lozano Garzón, “Análisis comparativo de tecnologías inalámbricas para una solución de servicios de telemedicina,” *Ingenieria y Desarrollo*, no. 25, pp. 200-2017, 2009. [Online]. Available: https://www.redalyc.org/pdf/852/85212371012.pdf

[15] P. Gomez and P. Angel, “Estudio de factibilidad para la implementacion de una red de sensores ambientales inalambricos para el riego de las areas verdes del complejo universitario de la Universidad Estatal del Sur de Manabi,” Tesis de Grado, UNESUM, 2019. [Online]. Available: http://repositorio.unesum.edu.ec/handle/53000/1542

[16] Network Working Group. Mobile Ad hoc Networking (MANET), 1999.

[17] B. SIG Working Groups. Bluetooth Core Version 4.2., 2014.

[18] A. M. Tablado, “Seguridad en Bluetooth,” Tesis de Grado, Universidad Pontificia Comillas, Madrid, 2006.

[19] A. Chaturvedi and M. Murthy, “WPAN scheme for Bluetooth devices: a review,” in *4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings*, 2003, pp. 5-7. [Online]. Available: https://ieeexplore.ieee.org/document/1188290

[20] Bluetooth SIG Working Groups. Bluetooth Network Encapsulation Protocol (BNEP) Specification, 2001.

[21] Apple. Posibles fuentes de interferencias de Wi-Fi y Bluetooth, 2016. [Online]. Available: https://support.apple.com/es-es/HT201542

[22] Wilysis. 2018. Network Cell Info Lite. [Online]. Available: https://play.google.com/store/apps/details?id=com.wilysis.cellinfolite&hl=es_41

[23] Ookla. Speedtest.net. [Online]. Available: https://play.google.com/store/apps/details?id=org.zwanoo.android.speedtest&hl%20=es

Información de Contacto de los/as Autores/as:

Andrés Gustavo Díaz
9 de Julio 317, La Banda
Santiago del Estero
Argentina
andy.sde@gmail.com
www.linkedin.com/in/andres-diaz-sde
ORCID: https://orcid.org/0000-0003-1038-3837

Lic. Fernando Raymundo Lazo
Catamarca 59, La Banda,
Santiago del Estero
Argentina
ferulazo@gmail.com
ORCID: https://orcid.org/0000-0003-2440-6569

Dra. Susana Isabel Herrera
Las Rosas 3434
Santiago del Estero
Argentina
sherrera@unse.edu.ar
www.linkedin.com/in/susana-herrera-b77406157/
ORCID: https://orcid.org/0000-0003-1462-6517

Dr. Sergio Hernán Rocabado Moreno
Pueyrredón 363
Salta
Argentina
srocabado@di.unsa.edu.ar
ORCID: https://orcid.org/0000-0003-1182-0592

Andrés Gustavo Díaz
Licenciado en Sistemas de Información de la Universidad Nacional de Santiago del Estero. Actualmente Administrador de Sistemas, Redes y Seguridad Informática en Compañía de Recreativos Argentinos UTE.

Fernando Raymundo Lazo
Licenciado en Sistemas de Información de la Universidad Nacional de Santiago del Estero. Actualmente Administrador de Redes Informáticas y servidores en Ministerio Publico Fiscal de Santiago del Estero y Profesor en Col. Privado de Beltrán.

Susana Isabel Herrera
Doctora en Ciencias Informáticas, Máster en Ingeniería del Software, Especialista en Docencia Universitaria, Licenciada en Sistemas de Información. Actualmente, Profesora e Investigadora de la Facultad de Ciencias Exactas y Tecnologías, UNSE.

Sergio Hernán Rocabado Moreno
Doctor en Ciencias Informáticas, Magister en Redes de Datos, Licenciado en Análisis de Sistemas. Actualmente, Profesor en la Facultad de Ciencias Exactas, UNSa e Investigador del Instituto de Inv. en Energía No Convencional.