Celik *et al. Applied Network Science* (2019) 4:102
https://doi.org/10.1007/s41109-019-0220-6

Applied Network Science

REVIEW Open Access

5G device-to-device communication security and multipath routing solutions

Aslihan Celik[1†], Jessica Tetzner[1†], Koushik Sinha[2] and John Matta[1*]

*Correspondence: jmatta@siue.edu
†Aslihan Celik and Jessica Tetzner contributed equally to this work.
[1]Southern Illinois University Edwardsville, Edwardsville, IL, USA
Full list of author information is available at the end of the article

Abstract

Through direct communication, device-to-device (D2D) technology can increase the overall throughput, enhance the coverage, and reduce the power consumption of cellular communications. Security will be of paramount importance in 5G, because 5G devices will directly affect our safety, such as by steering self-driving vehicles and controlling health care applications. 5G will be supporting millions of existing devices without adequate built-in security, as well as new devices whose extreme computing power will make them attractive targets for hackers.

This paper presents a survey of the literature on security problems relating to D2D communications in mobile 5G networks. Issues include eavesdropping, jamming, primary user emulation attack, and injecting attack. Because multipath routing emerges as a strategy that can help combat many security problems, particularly eavesdropping, the paper contains an extensive discussion of the security implications of multipath routing. Finally, the paper describes results of a simulation that tests three path selection techniques inspired by the literature. The simulation reveals that routing information through interference disjoint paths most effectively inhibits eavesdropping.

Keywords: Cellular networks, 5G, D2D communications

Introduction

5G networks are expected to be deployed by 2020 (Ge et al. 2014), and by the year 2030 nearly 60 percent of the world's population will be living in urban environments (AlDairi and et al. 2017). Due to the increasing number of mobile devices in cities, 5G is expected to play an important role in the development of smart city applications (Gharaibeh et al. 2017). 5G offers great promise, potentially giving individuals the opportunity to communicate with whomever they want whenever they want in the context of a "human-centric system" (Skouby and Lynggaard 2014). Device-to-device (D2D) is a radio communication technology that allows devices to directly exchange data without the need for base stations or access points (Gharaibeh et al. 2017).

5G wireless systems are expected to connect various "smart" objects within Smart Homes and Smart Cities as well as to monitor information from the surrounding environment. One problem is that cellular communications generally require high energy consumption. Implementing a large scale Internet of Things (IoT) in a Smart City with D2D communications is viable due to the efficient use of radio resources and low energy usage that characterizes D2D (Orsino et al. 2016).

An extensive survey on issues involving wireless security is given by Zou et al. (2016). Security will be of paramount importance in 5G networks, because 5G devices will

directly affect our safety in urban environments, such as by controlling self-driving vehicles, traffic lights, utilities, and personalized health care appliances. 5G will also be supporting millions of devices that already exist without adequate built-in security, as well as new devices whose extreme computing power will make them attractive targets for hackers (Schneider and Horn 2015).

In the United States The FCC Technological Advisory Council gives guidelines as to four recommendations for security in 5G (McGarry). First, it is recommended that 5G be implemented such that denial of service (DoS) attacks are thwarted through resource isolation, authorization restriction and embedded DoS detection and mitigation functions. The second recommendation is that D2D communications provide for privacy by using asymmetric key based encryption with safeguards to prevent identification of users based on keys. Third, it is recommended that strong identity management that can identify and authorize users entering a network be implemented. The final recommendation is that resource isolation techniques be used to enable different security levels for different resources.

Wang and Yan (2015) enumerate the security requirements of D2D networks. These include not only the CIA triad of confidentiality, integrity, and authentication, but also privacy, non-repudiation, revocability of access, and availability and dependability of the network. The way these issues are addressed in 5G will differ from conventional wired and even wireless networks, primarily because of four characteristics of D2D communication, as given by Abualhaol and Muegge (2016). First, the airwaves are shared and freely accessible. Second, a D2D network is made of mobile devices and thus is constantly changing. Third, network architecture is open, and fourth, resources in terms of bands and channels are limited. Four overarching types of attack are possible: eavesdropping, jamming, restricting access, and injecting. Each of these attacks is similar to attacks that could occur on wired networks (or the internet), but they manifest themselves differently because of the unique properties of D2D communications in 5G.

Mitigation of security threats is an ongoing concern. Many conventional approaches exist, such as use of encryption. In this paper we present a graph theory approach to preventing eavesdropping – sending data simultaneously along multiple paths. This is a good strategy in crowded city environments, because multiple paths are likely to exist, many devices are likely to be low power or have low processing capabilities, and potential eavesdroppers are numerous. We test and compare three different multi-path relay strategies (generally used for load management or non-security purposes) for their resistance to eavesdroppers. This is accomplished by running a simulation using Davies's "City Section Mobility Model" (Davies and et al. 2000), an abstraction of how people and devices move in the city.

The rest of the paper is organized as follows. We begin with an extensive survey of security threats in 5G networks. In particular, we cover four types of attacks in the "Review of D2D security threats" section, which includes sections concerning "Eavesdropping," "Jamming," "Restricting access: primary user emulation attack," and "Injecting attack" sections. Because our simulations involve multipath routing, we follow with a review of "Multipath routing and corresponding security implications" section. We then present our work on "Using multipath routing to thwart eavesdropping" section, which includes "Overview", "Secure multipath routing related work", "Methodology", and "Results" sections. Finally, a "Conclusion" section finishes the paper.

Review of D2D security threats

Eavesdropping

Eavesdropping involves an intruder listening to an exchange of information, which, depending on the nature of the information and the abilities of the intruder could take many forms. In one example, it is revealed that the sound of people filling out medical forms could be overheard by mobile devices, which could then be used to decode sensitive information (Yu et al. 2016). Zhang et al. note that, in a relay situation such as would exist with 5G D2D communication, the relaying node can be thought of as an eavesdropper from whom data must be hidden, even though it is essential to the transmission (Zhang et al. 2010). Other specific challenges and opportunities arise because of the nature of 5G systems, which have open architectures, are large and consist of many nodes with different security needs, and will be implemented via a massive Multiple-Input Multiple-Output (maMIMO) physical layer that offers new spectral and energy efficiency benefits.

The openness of wireless network architecture facilitates eavesdropping. One of the most important protections against it is cryptography, as it is more difficult to listen in on an encoded message. Cryptography requires senders and receivers to calculate and exchange keys (Sarma and Kuri 2015). By their nature, cryptographic solutions rely on the limited computing power of the eavesdropper and the hardness of breaking (or intercepting) a key (Zou et al. 2016; Fang et al. 2018). A criticism of this approach is that changes in technology, such as advances in quantum computing or the discovery that P=NP could make decoding encrypted messages possible (Schneider and Horn 2015). Cryptography remains a potent defense against eavesdropping in a 5G environment, in part due to many lightweight cryptography implementations that can be run even on devices with low computation or energy resources (Eisenbarth et al. 2007). Sun and Du remark on the "binary" nature of cryptographic solutions – the key is either intercepted or it is not (Sun and Du 2017). They also note that different applications may require different degrees of security, which cryptography cannot provide. For example, financial transactions require more security than web browsing.

Also, even if an eavesdropper cannot intercept a received signal directly due to encryption, traffic analysis can be used in a passive attack, where an eavesdropper intercepts information such as the location and identity of the communicating parties by analyzing the patterns of the received signal without understanding the content of the signal itself (Fang et al. 2018).

Eavesdropping can manifest in different forms. In a report on 5G risk assessment (Naslund et al. 2016), it is apparent that widely different types of information can be eavesdropped and used maliciously for many different purposes. The problem is likely more pervasive in the 5G domain, which differs from even the domain of 4G devices. The 5G domain may contain 3rd-party ID providers, such as home networks, and infrastructure domains such as transit networks and cloud providers. For example, information on nodes that have recently joined a network can be used to track a user's location. The authenticating node itself can act as a man-in-the-middle, and can use the information gained from authentication to "provide tampered security configurations." It is possible that information being sent to and from a centralized control plane may be more interesting to an eavesdropper than the actual private data, and in any case can be used to reroute that data in a malicious manner. Even a seemingly innocuous smart home (Porambage et al.

2016), with simple devices sending information about lighting and heating and the operation of the refrigerator, can become a source for attack if the timestamps on the messages give an attacker useful information, such as when the occupants of the house are away, or sleeping. It is noted that this may result in a lack of trust in IoT devices and 5G networks in general.

Eavesdropping can be modeled as a simple problem, where transmission channels are used by three parties: a source node, a destination node, and an eavesdropping node. The ideas for combating eavesdropping center around creating a better source-to-destination channel, and/or jamming or interrupting the source-to-eavesdropper channel.

Eavesdroppers can be seen as active or passive. Passive eavesdroppers simply monitor activity and do not have any direct effect on the network. Active eavesdroppers, however, send their own messages to mimic those of legitimate users (Kapetanovic et al. 2015). Xu, Duan and Zhang introduce a type of active eavesdropping called proactive eavesdropping. They categorize eavesdropping as legitimate and illegitimate. Proactive eavesdropping aims to attack authorized third parties such as government agencies via legitimately monitoring suspicious communications for crimes and terror attacks (Xu et al. 2017a). According to Xu et al., there are three methods to implement proactive eavesdropping for surveillance purposes by using existing wireless infrastructures such as cellular base stations and WiFi access points. These methods are "jamming," "relaying," and "jamming the suspicious transmitter" (Xu et al. 2017b).

Closed access means that entry to a network is restricted. The combination of closed access and encryption offers protection against eavesdropping, and is the anti-eavesdropping method used by many wireless networks. Wang and Yan note that in 5G systems *open access* may more often be the case due to the lack of authentication in the macro cell or the micro cell tiers (Wang and Yan 2015). They also note that the maMIMO design of D2D networks uses a reduced transmit power level. This means that eavesdroppers must be closer in order to receive a signal, which obviously makes eavesdropping more difficult. On the other hand, they also note that data can be eavesdropped and manipulated through lawful interception channels (that is to say, the network has a built-in capability to be listened to). Each user is basically "an eavesdropper for all messages other than its own."

Kapetanovic, Zheng and Rusek point out that physical layer security (PLS) against passive eavesdropping attacks is a built-in advantage of MaMIMO systems, and therefore of 5G networks. "With standard time-division duplex (TDD) mode MaMIMO operations, the received signal power at the legitimate user is several orders of magnitude larger than the received signal power at the eavesdropper" (Kapetanovic et al. 2015). An eavesdropper can counteract this by placing himself closer to the user. Also, the eavesdropper can become active by sending a message to the base station pretending to be the legitimate user, which will cause the base station to beamform signal power to the eavesdropper instead of the legitimate user. MaMIMO is not resistant to active eavesdropper attacks, which makes it important to be able to detect an active eavesdropper. The paper (Kapetanovic et al. 2015) presents 3 schemes by which an active eavesdropper can be detected. Two involve "legitimate users transmitting a sequence of random phase-shift keying (PSK) symbols, which form the key to detecting the eavesdropper at the base station." The base station computes a detection statistic which converges to a "phase of a valid PSK symbol" if an active eavesdropper is not present, and does not converge otherwise.

The beamforming capability of the base station can also be used to detect an eavesdropper. The user sends the base station a training signal, and the base station beamforms based on it, sending a signal "which ensures that the received signal at the legitimate user after processing becomes 1." This means that the signal received by the user is secure. If it is a smaller number, the beam is being directed to an eavesdropper, who is detected.

An alternative approach to detecting active eavesdroppers is to attempt to thwart all eavesdroppers by introducing interference into the messages being transmitted. Sarma and Kuri describe a scheme where devices cooperate to do low level jamming with artificial noise transmission (Sarma and Kuri 2015). This involves transmitting across a multi-hop network with multiple eavesdroppers, a situation where security is assured by a high signal-to-interference-plus-noise ratio (SINR) at sender and receiver nodes, and a low SINR at eavesdropping nodes.

A widely studied way to prevent attacks is through physical layer security. According to Cumanan et al. physical layer security is being analyzed specifically in the context of device-to-device networks (Cumanan et al. 2017). Physical layer security exploits the characteristics of a wireless channel to prevent eavesdropping and other attacks. According to Sun and Du (2017), this is much more efficient because no data has to be encrypted when devices communicate. Specifically, in a 5G network with many devices connecting, it would be hard to manage and define the mass amount of encryption keys that would be necessary to encode the data. By exploiting the physical aspects of a channel, devices can communicate faster because they do not have to handle encryption. Another benefit of using physical layer security, according to Xie and Zhang (2018), is the fact that a receiver would be able to quickly tell if an attack was going on without having to use high processing power.

Physical layer security uses characteristics of a channel, like noise, fading, and interference to ensure communication between devices is secure. According to Alavi et al. (2017), this is entirely dependent on being able to access all of the channel state information perfectly. If the information is not accessed correctly, regular channel use could be misinterpreted. Another method of preventing attacks using physical layer security in D2D networks proposed by Yang et al. (2015) is making a closed access system for devices that communicate directly with other devices. This means that each device has a list of trusted devices. If an unlisted user wants to contact the initial user, they must first be authenticated by the initial user. They note that closed access may not always be implemented in a 5G network, "due to the lack of authentication in the macro cell or the micro cell tiers."

Mucchi et al. suggest a way to detect an eavesdropper without knowing its location. Their technique is called secrecy pressure (Mucchi et al. 2017). Secrecy pressure measures how secure a link in a communication path is based off its environment. The authors derive an equation to measure the pressure by accounting for the distance and the angle of the antennas that are used for communication. Using this equation, they determine the optimal position for the antennas. This metric differs from others because nothing is based on the position of the eavesdropper. The eavesdropper can be anywhere in the range, and the equation will still find optimal antenna positions that decrease the eavesdropping rate.

Another way to combat attacks uses jamming to interrupt eavesdropping. Though jamming is commonly thought of as a negative action, here it can be used to ensure that information is secure. Jiang et al. (2015) propose a technique called cooperative jamming

that uses physical layer security. According to Jameel et al. (2018), cooperative jamming occurs when a node creates interference for an eavesdropper, effectively keeping the information that would have been intercepted secure, as well as confusing the eavesdropper. Zhang et al. also identify cooperative jamming as a promising approach (Zhang et al. 2010), mentioning that because the initial user knows that a jamming interference will occur, they are easily able to accommodate the interference. Another type of jamming, according to Huo et al. (2018), is called directional jamming. In directional jamming, the noise is sent out in a single direction. This is most effective if the eavesdropper's location is known.

Jamming

A property of 5G networks is *opportunistic spectrum access*, which means that secondary users sense spectrum vacancies and utilize that spectrum while not interfering with its primary users (PUs). One side effect is that frequencies are subject to jamming. Jamming is the malicious insertion of noise or signals into a channel in order to prevent the channel's use.

Li and Cadeau study both the jamming capabilities of some actors in a cognitive radio network, and the anti-jamming capabilities of others (Li and Cadeau 2011). They identify three jamming strategies. Under *strong jamming*, a transmission is completely disrupted. To escape strong jamming, sender and receiver must switch to an unjammed channel. *Light jamming* injects enough interference to make a user assume the interference is caused by a primary user and switch channels. *Smart jamming* jams only the control signals.

Lichtman et al. assess the threat and mitigation of jamming specifically in 5G networks. One 5G property that mitigates jamming is its wide range of frequency use. Specifically, using frequencies greater than 24GHz inhibits jamming, because of the difficulty of building a jammer for cells operating above 24GHz (Lichtman et al. 2018). In 5G networks Primary and Secondary Synchronization Signals (PSS and SSS) are control signals which allow a device to identify base stations with low SINR. This makes them resilient to jamming because it requires an attacker to use "more jamming power to successfully jam the signal" (Lichtman et al. 2018).

Techniques that spread signals over a wider bandwidth such as *direct sequence spread spectrum* (DSSS) and *frequency hopping spread spectrum* (FHSS) are used in 5G networks to act against jamming at the physical layer (Fang et al. 2018). In general, schemes that utilize hopping rely on sharing a key between sending node and receiving node. How this can happen in an open environment with potential jamming is a difficult question, because the key propagation depends on communication, and communication depends on key propagation. This is referred to as the anti-jamming/key-establishment dependency. In Strasser et al. (2008), propose to break this dependency using a scheme called Uncoordinated Frequency Hopping (UFH). In UFH, potential senders and receivers hop along randomly chosen frequency channels, with the sender sending partial messages at each frequency. UFH is especially interesting because it also guards against injecting attacks if each part of the message received contains a hash that points to the next part of the message.

An anti-jamming protocol for cognitive radio networks is proposed by Bhattacharya et al. (2016). In this protocol, both sending and receiving nodes share knowledge of a

randomly-generated sequence of channels, generated based on a shared key. If the receiving node senses that it is jammed, it sends a *jammed* message to the sending node, which is not jammed and is therefore able to receive it. The receiving node may also detect a collision between the jammed signal and the signal from the sending node, in which case it sends a *collision* signal. After some pre-agreed number of jammed or collision messages, both parties switch to a new, mutually known channel. If the sender is jammed, it sends *move-to-next-channel* requests instead of data. The receiver can hear this request, and send an acknowledgement (ACK), which cannot be received by the sender due to jamming. However, after some number of messages are sent during a number of time slots, both parties switch to a new channel, unknown to the jammer. When both are jammed, they perform similarly to the first two cases, and switch channels after a time.

Another frequency-based model is proposed by Su et al. (2011). They assert that a weakness of models where new channel assignments are preknown is that a jammer potentially has access to the same information. In their model, both sender and receiver use learning to determine which channel to switch to. Here, both sender and receiver are given a *multi-armed bandit* (MLB) algorithm. Based on successful outcomes, both parties learn to sense which channel the other will pick.

Adem, Hamdaour and Yavuz propose time-based hopping instead of frequency-based hopping (Adem et al. 2015). In this scheme, a channel is divided into n portions, and data is sent by a user over one portion. Time is divided into slots (for example, enough to send one packet), and users switch continuously between slots based on a predetermined random sequence. In Adem et al. (2016), Adem, Hamdaoui and Yavuz expand their work from Adem et al. (2015), and offer two additional takes on time-based hopping schemes, applicable when users are mobile instead of stationary, and when there is access to an arbitrary number of channels (even only one). These cases more accurately represent the reality of 5G D2D communications. In these schemes "a user transmits some data over some time, holds for some other random amount time, and then transmits again and so on," with the goal of making the actual transmissions look random to a jammer. In Private Key Based Time Hopping (PKTH) a trusted third party is used to handle key distribution. With Selective Diversity Based Time Hopping (SDTH) some method (chosen by the implementer of the protocol) is used to assess the quality of available channels and the highest quality channel is selected.

Game theory can provide insight into anti-jamming algorithms. The situation of jamming, where users want to employ a frequency and jammers want to prevent access, can be viewed as a zero-sum game. The game described by Wu et al. (2012) is formed such that senders and receivers use a channel, and at the end of a time period decide to either hop (in the case of jamming) or stay.

Restricting access: primary user emulation attack

The idea of Primary User Emulation Attack (PUEA) is similar to jamming, as it attempts is to create a situation where a user will decide not to use a channel. It is one form of a Denial of Service (DoS) attack. In the case of PUEA, the secondary user (SU) senses that the channel is in use by its primary user, and so does not consider using it. This type of attack is effective because of a "listen before talk" (LBT) spectrum etiquette (Jin et al. 2016). PUEA is, in particular "the DoS attack that 5G networks are susceptible to," because with unlicensed spectrum, malicious users aren't easily identifiable (Jin et al. 2016).

The security issues surrounding PUEAs in 5G networks are comparable to those of a cognitive radio network (CRN). According to Fauzi and Khan (2017) being aware of the current issues in CRN security will allow for an easier deployment of 5G networks. The authors categorize PUEAs into Greedy/Selfish and Malicious. A greedy attack is when the attacker emulates the PU's signal so the channel is cleared. Malicious attacks are when the PU's signal is emulated to cause a DoS attack. By analyzing the security issues in CRNs, countermeasures can be taken to combat the potential security issues in 5G networks.

There are several ways to combat PUEA, categorizable as location aware and location unaware. "Typically, location aware techniques involve significant infrastructure overhead like a dedicated sensor network to determine the locations of transmitters" (Jin et al. 2010). Different ways of identifying this type of attack are proposed by Chen and Park (2006). The goal of distinguishing licensed versus PUE signals is accomplished through a location verification scheme. The paper describes two techniques that can be used for location verification: the Distance Ratio Test and the Distance Difference Test. Distance tests (of both sorts) are based on the correlation between the length of a wireless link and the received signal strength.

It is noted in Jin et al. (2016) that PUEA attacks are interesting from a graph theoretic point of view because they remove nodes from the D2D network, potentially disconnecting it. And it's not just senders and receivers, but also the relays they rely on that can be affected. They provide some calculations on the actual damage that a PUEA can cause. "For a small network (a network with 100 secondary users or less), a 5% probability of successful DoS attack results in a significantly large (more than 20%) probability of disconnecting a connected ad hoc network." Empirical results show that with individual nodes making individual decisions to leave a channel, the probability of network disconnection is as high as 70%.

One individual and one centralized method are described by Jin et al. (2010). With the individual method, each secondary user senses and measures its received power. If received power falls within a statistically predicted range, the channel is determined in use by a PU, otherwise it is determined to contain a PUEA. In the centralized version, each node in a network sends its sensing result to a centralized controller that determines if a PUEA is detected.

In addition to Jin et al. (2016)'s statistical approaches, there are ideas based on signal strength (Chen et al. 2008), and also primary transmitter location. Chen and Park propose a *Distance Ratio Test* (Chen and Park 2006). As with previous methods, individual users measure signal strength on a channel. Here, however, a pair of nodes act as "verifiers" which test a calculated location against the PU transmitter's known location. The second technique, *Distance Difference Test*, relies again on the signals observed by a pair of verifiers, but this time uses the detection of the phase difference of the primary user's signal to deduce the correctness of the transmitter's location. Huifang et al. (2014) propose a scheme for cooperative spectrum sensing based on the realization that, when sensing PU signals, nodes close together will get substantially the same result. So, it divides the entire network into closely-located clusters, and each cluster reaches a decision independently, which is then communicated to a central authority.

Another scheme is the two-phase INCA (deceNtralized Cooperative Analysis), proposed by Soto, Queiroz, Gregori, and Nogueira in Soto et al. (2013). The two phases are individual analysis and cooperation. The individual analysis phase employs NWAUF

(Normalized Weighted Additive Utility Function). This scheme is not bound to an individual type of data, but can be adjusted to fit data that become relevant. "An arbitrary node samples each criteria and starts the NWAUF analysis." All nodes in the network complete this analysis, and in the cooperative phase share their results with each other. Each SU node conducts "a conditional probability analysis to determine the probability of the presence of a PUEA in the network." This method is interesting because each node effectively makes its own decision about whether there is a PUEA, without any central authority being involved, and decides thereafter whether or not to occupy the channel in question.

A good survey article on various other approaches to thwarting PUEA is at Das and Das (2013). Also, see Naqvi et al. (2013) for a survey with taxonomy of different types of attacks.

Injecting attack

In the injecting attack, data is not just eavesdropped, and channel use is not just interrupted, but data is actually maliciously changed. Such attacks go under various names and subgroups such as data manipulation attack, relay attack, hijacking, rerouting, man-in-the-middle, intrusion detection, signal insertion attack and spectrum sensing data falsification. It would seem obvious, that in a situation where relay is common, a man-in-the-middle attack would also be common. Secondary users in ad-hoc mobile networks have no reason to trust their relaying nodes. Cryptography and authentication are often mentioned as ways to thwart injecting attacks. This means that keys must be exchanged in a secure fashion.

In Sedidi and Kumar (2016) discuss three key exchange protocols. Each protocol involves two users and a base station. Two channels, a public channel and an encrypted, dedicated channel are both used. Communications between the two users are managed by the base station, and among the three protocols the most secure involves a greater number of computations by the base station. Thus, security can be traded for computational simplicity. These protocols work because the encrypted channel is the link between the users and the base station, which makes it unidentifiable to a man-in-the-middle attacker.

The use of authentication is addressed in Abualhaol and Muegge (2016), through the issue of continuous authenticity and legitimacy patterns. One-time authentication leaves a link vulnerable. They propose verifying through a legitimacy pattern, which is bits contained in a packet that enable the recipient of the packet to detect physical layer attacks in a wireless channel. The legitimacy pattern is able to be verified through three attributes transmitted along with each packet: pattern size, location and value. It is noted that eavesdropping is the only type of attack that cannot be detected by continuous authentication.

Three more types of injecting attacks are introduced in Khan et al. (2017). These attacks are the replay attack, in which valid data is repeated maliciously, Denial of Service (DOS) attack which blocks access to available resources, and the interleaving attack, which is an attack on an authentication system that lets the attacker derive authentication information from the legitimate communication.

The application layer manages interactions with the end user, and physical layer security lacks the ability to prevent application layer attacks, such as hacking sensitive information stored in devices, like authentication keys or credit card information (Pedhadiya et

al. 2018). Intrusion detection system (IDS) is an alternative to detect and report malicious attacks within its detection area by providing surveillance on network traffic, system logs, running processes, application and system configuration changes, file access and modification (Borges et al. 2017).

Multipath routing and corresponding security implications

Metrics for multipath routing

Multipath routing in radio networks is an interesting and difficult problem. Yang et al. (2005) discuss that, because of shared airwaves and interference (and the static nature of nodes), routing requirements are different than for wired or other networks. The best metric for evaluating different routes depends on the goal of the network, which might be speed, reliability, secrecy, or energy efficiency. Characteristics that impact the performance of a path are path length (shorter preferred), capacity, data loss ratios, and interference. Nodes not only use bandwidth with their own transmissions, but also interfere with nodes that are close by. Interflow interference is the interference that results when *two different flows* attempt to use (or interfere on) the same channel at the same time. Intraflow interference is what results when two parts of the same flow attempt to use (or cause interference on) the same channel at the same time. Capturing and quantifying interference when quantifying the efficiency of routes is difficult because both the channel used by the link and the capacity of the link are related to the interference that the use of the link imposes on its neighborhood (Yang et al. 2005).

Isotonicity is a property of a routing metric, and is a necessary property for that metric to be used successfully with shortest-paths algorithms. In general a routing method is isotonic if the order of its weightings holds when the paths are appended or prefixed by a common third path. Mathematically, where $W(i)$ represents the length or weight of path i, $W(a) \leq W(b)$ implies both $W(a \oplus c) \leq W(b \oplus c)$ and $W(c' \oplus a) \leq W(c' \oplus b)$, for all paths a, b, c, c', where path concatenation is represented by $\oplus$. If a metric is isotonic, Dijkstra's and Bellman-Ford's algorithms can be used to find optimal paths, and circular paths will be avoided. The best metrics will allow these algorithms to find the shortest, highest-throughput, lowest-interference paths between source and destination.

Cikovskis and Slaidins (2015) discuss the problems inherent in finding multiple possible paths. Multiple paths require more information, and more memory and storage in routing tables. Once discovered, actual paths to be used must be chosen, requiring computing power. Interference must be taken into account when choosing usable routes. Once routes have been chosen, a strategy for distributing the data among paths must be chosen (for example, round robin distribution of packets). How can different path sets be evaluated? One metric is by how separated they are. This is "difficult to determine because geometry of path sets is complicated and there is no common approach how it should be measured" (Cikovskis and Slaidins 2015). They use average distance between nodes of both paths:

$$d_{pq} = \frac{\sum_{n \in p} d_{nq}}{hops(p)}. \tag{1}$$

Here, the distance between node n in paths p and q equals the minimum distance from node n to any node m in path q:

$$d_{nq} = min_{m \in q}(d_{nm}). \tag{2}$$

Yang and Tang (2014) show that because of omnidirectional transmissions, a node-disjoint path is better than an edge disjoint path (because in a node-disjoint path "no edge or node is likely to become a bottleneck"), and still, because of intra- and inter-path interference, a strategy that only chooses node-disjoint paths is not enough. A better strategy minimizes intra-path interference by using an *irreducible* path. In an irreducible path, there's no common neighborhood among two subsequent nodes along a path. Each link interferes only with its adjacent links. Because of this lack of interference, the path cannot be made longer (by branching out to an interfering node and back to the original path). A second type of disjointedness is a neighbor-disjoint path. This path has no inter-path interference. There are no links between any intermediate nodes in two neighbor-disjoint paths. The optimal path that reduces all interference is the irreducible and neighbor-disjoint path. They go on to prove that "irreducible and neighbor-disjoint paths can provide near-capacity throughput for multiple-path transmission as long as there're sufficient number of them."

Disjoint paths, graph coloring and conflict graphs

In a D2D network, reliability is an issue, as nodes are constantly entering and leaving the network. Relying on a single node or series of nodes is potentially disastrous, if the node leaves the network or becomes disabled through interference. As Kuperman and Modiano point out, "Switching to a backup path after some failure may cause interference with already existing paths, disrupting connections that were not affected by that failure" (Kuperman and Modiano 2014). The answer is to send data across multiple paths, and preferably disjoint paths. Then disruption on one path will not affect the others. Selecting the shortest paths does not necessarily work for this purpose, as selection of the first path may prevent finding of further disjoint paths.

In its simplest form, a conflict graph can be used to minimize interference between primary and secondary users, as well as the interference between secondary users. Tushir et al. (2016) discuss a Graph Coloring based Dynamic Channel Allocation (GC-DCA) model. A communication graph is constructed where nodes i and j have a link if they have at least one of the same channels on their channel lists, and if they are within transmission range of each other. A conflict graph is constructed which keeps track of different types of conflicts, such as the fact that if one secondary user (SU) is linked to two or more SUs, conflicts could occur if both links try to communicate to the first SU at the same time, and if two sets of SUs try to communicate on the same channel their transmissions could collide. The different conflicts are weighted by SINR, and the graph is colored by channel.

Disjointedness can take many forms. As the most simple example, any transmissions across a D2D network must be interference disjoint. One way of preventing generalized interference is through the use of a conflict graph. The idea is discussed by Teotia et al. (2015). The edges of a D2D network become the nodes of a conflict graph. Edges that are within range of each other are noted as conflicting by adding a corresponding edge to the conflict graph. If this graph is then colored, with channels as the colors (or assigned channels through a simple breadth first search), the resulting channel assignment guarantees lack of interference. This concept can be generalized for different types of conflicts. For choosing broadcast-range disjoint paths, the conflict graph can be constructed to identify all nodes within broadcast range. Because interference implies the ability to eavesdrop, selecting interference-disjoint paths and sending different chunks of a message down

different paths can prevent the ability of a single node to eavesdrop on a transmission. According to Wu and Zhang, constructing a conflict graph requires base station coordination, and is an iterative process requiring interpretation of messages and ACKs (Wu and Zhang 2014).

Plummer et al. use conflict graphs to develop an algorithm that is capable of dynamic channel assignments and can be computed in a distributed fashion (Plummer et al. 2007). In their Cognitive Spectrum Allocation Protocol (CoSAP), each node computes its own routing table for up to m-hop neighbors by sending availability over a common control channel. After creating a connectivity graph, each node can use this information to create a channel conflict graph for each channel, where for a given channel, a transmission becomes a vertex in the conflict graph. If two channel vertices are within radio transmission range and can interfere, an edge is added to the conflict graph. The degree of a vertex is therefore the amount of expected interference on a channel. The channel with the lowest degree is chosen for transmission.

Yu and Liang propose a scheme called DNDR (Dual Node-Disjoint Paths Routing) (Yu and Liang 2015), where the routing table of each node keeps not just a first but also a second route to each destination, meaning that there are always two choices for the next hop. Data is transmitted via the primary route, moving to the secondary route in cases where a link disconnection is encountered.

Interference in multipath routing

Thulasiraman et al. (2011) add interference constraints to the problem of multipath protocols. They rely on the Quality of Service (QoS) concept of "max-min fairness," which implies developing a metric that will prevent starvation of a flow, and at the same time increase the bandwidth of a flow. Menger's Theorem is a variation on min cut / max flow and says that the maximum number of disjoint paths between nodes s and d is the minimum size of the cut that disconnects them. The interference-aware metric, called the Routing with Interflow and Intraflow Interference Metric (RI^3M) is expressed mathematically as

$$RI^3M = \sum_{\forall (i,j) \in p} IL_{ij} + \sum_{\forall i \in p} CSC_i, \tag{3}$$

where i is a node, and i, j is a link, both along path p. The components of this equation, IL deals with interflow interference and load awareness, and CSC (channel switching cost) captures intraflow interference. CSC gives paths with consecutive links using the same channel a higher cost than paths that alternate their channel assignments, which means it favors more highly diversified paths. RI^3M used by itself is not isotonic, but can be made isotonic using a virtual network decomposition technique. The network is relatively easy to decompose because of the limited choices: a path only becomes non-isotonic by the addition of a node on the same channel, and the selection of channels that can be added is limited. When the graph has been decomposed, any shortest-distance algorithm can be run on it. Suurballe's algorithm is recommended for finding two disjoint paths.

Many of the issues of interference mitigation in D2D communications are discussed by Safdar et al. (2016). Several interference avoidance techniques follow. Power control (PC) techniques lower the power of transmissions to prevent interference. These

techniques work best when devices are close – the power of the transmissions need only be great enough to get the signal from one to another. PC is not always applicable. If power levels are too low, it severely restricts the number of nodes that can be included in the network. Radio resource allocation techniques assign channels such that nodes do not interfere with each other. This will impose significant overhead if the channels are assigned by a base station. More sophisticated algorithms attempt to leverage both power control and resource allocation in a combined fashion to prevent interference. Time division multiplexing splits the spectrum over time, but can lead to inefficient use of resources. It is thought that Multiple-Input Multiple-Output (MIMO) antenna systems can use beamforming techniques to limit interference.

Safdar et al. give one reference to an interference mitigation technique between multiple D2D users called greedy orthogonal resource allocation. Orthogonal by definition describes resources that do not interfere with each other. Xu et al. discuss interference mitigation in the context of improving the overall system capacity and spectrum efficiency of the network (Xu et al. 2013). Neighbors in a network should be assigned orthogonal channels to prevent interference. The answer is to design a neighbor set that minimizes resource wastage (because of all nodes being assigned orthogonal channels), while at the same time minimizing interference caused by same-channel transmissions. Assuming a certain QoS requirement means that there is a limited number of D2D communications that can occur within that neighborhood at a given time. D2D pairs are made into a graph by the base station, and colored based on channel assignment. The coloring creates an optimal channel assignment.

Le creates a multipath routing protocol (Le 2012) by modeling a network as a weighted directed graph. Interference is divided into 4 zones, based on intensity, or closeness to to a node. When total interference (all zones) is computed, a graph is created with edges based on the amount of interference. The status of each link is defined by information in transmitted messages. The weight of each link is the interference level of the corresponding link. Because the edges are weighted, Dijkstra's algorithm can then be used to find the path with minimum interference. Second and subsequent paths can be found again using Dijkstra's algorithm, but avoiding the nodes found in previous paths. This method does not necessarily find the optimal paths, but has the benefit of low computational complexity.

Multipath routing and security

Security in a D2D network involves transmission of keys and other sensitive data. When data is sent along a single path, the attacker must target only one node along the path. Use of multiple disjoint paths to send data means that an attacker must target many nodes. Multipath routing protocols can be based on min-cut/max-flow theory. The maximum number of disjoint paths that can be discovered between source S and destination D is equal to the min-cut between S and D.

Faisal and Mathkoor discuss a protocol for using multipath data transmission to improve security (SDTP: Secure Data Transmission Protocol) (Faisal and Mathkoor 2015). The use of multipaths is good for load balancing and transmission reliability, as well as for security. For route discovery they use a secure multipath algorithm called SecMR, which "discovers the complete set of the existing node-disjoint

and non-cyclic paths between a source and a destination node" (Mavropodi et al. 2007). In SecMR each node has both public and private security keys, which can be verified through a certificate authority. Use of keys helps to ensure confidentiality and integrity of data, as well as authentication of entrants to the network. SecMR prevents replay attacks through the use of timers. SDTP uses the keys created during route discovery to encrypt information, and divides the encrypted data into shares with some redundancy, based on the available number of paths. The shares are transmitted across the paths, and the data is reassembled at the destination.

Murakami et al. propose using disjoint paths to thwart eavesdropping (Murakami et al. 2015). The selection of disjoint paths is made more complicated in D2D networks, because it is not just the disjointness of nodes that is important, but also the disjointness of their broadcast ranges. If two paths are not broadcast-range-overlap disjoint, transmission on either path can be intercepted by the same eavesdropper. Notification messages are introduced to avoid overlaps. The scheme does not actually find multiple paths, but identifies overlaps in existing ones.

Using multipath routing to thwart eavesdropping

Overview

Ensuring secure communication between devices is especially important in high density environments like cities (Schneider and Horn 2015). It was noted previously that because interference implies the ability to eavesdrop, selecting interference-disjoint paths and sending different chunks of a message down different paths can prevent the ability of a single node to eavesdrop on a transmission (Teotia et al. 2015). Building on this idea, we have generated a simulation that tests three multipath routing algorithms to determine their utility in preventing eavesdropping attacks.

The network being studied is a D2D cellular network. The network is described as a connectivity graph, $G = (V, E)$ where vertices represent individual devices, and edges represent the ability of a signal to be transmitted between them. The vertices are cognitive radios, which are capable of transmitting and receiving over a series of non-overlapping channels. Edges occur where two devices are within a transmission range, and imply potential, not actual, transmissions. An example connectivity graph output from our simulations is shown in Fig. 1.

Our simulations are based on the findings of Murakami et al. (2015), in which eavesdropping is mitigated by sending data via relay nodes on two disjoint paths. Each node in a path is a potential eavesdropper. To most effectively mitigate eavesdropping, paths chosen must not only be node-disjoint, but also interference-disjoint.

Secure multipath routing related work

Use of mutipath routing for secure and reliable transmission of data has been extensively studied in the context of wireless sensor networks and multipath TCP (MPTCP) routing (Yang et al. 2014; Munir et al. 2017; Shafiq et al. 2013). Multipath routing has been used for improving packet delivery ratios by distributing load more efficiently (Wang et al. 2001; Ganjali and Keshavarzian 2004; Bhattacharya et al. 2018; Pearlman et al. 2000), improving energy usage efficiency (Ben-Othman and Yahya 2010; Velásquez-Villada and Donoso 2013), and dealing adaptively with congestion (Tran and Raghavendra 2005).

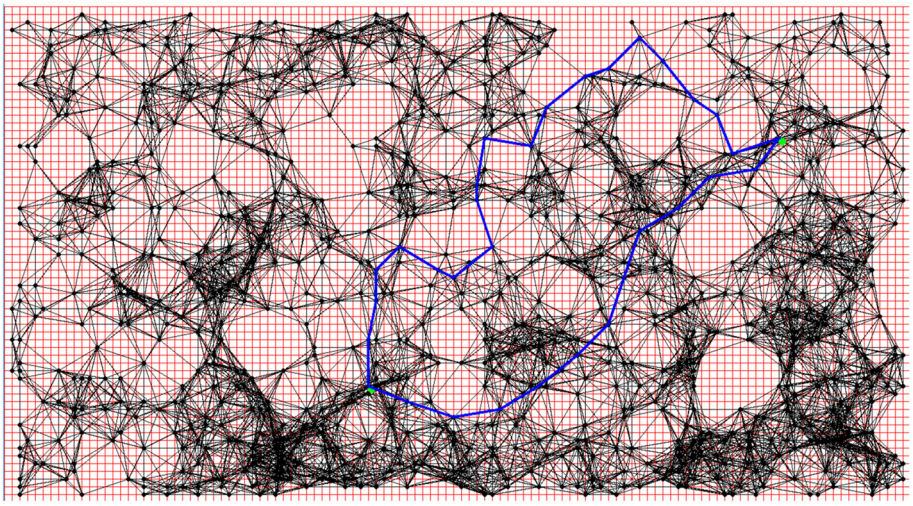

Fig. 1 Output From a Simulation. The city grid is represented by red lines. Black lines show that two nodes are within transmission radius. Source and destination nodes are shown in green, and two chosen paths are shown in blue

In the context of wireless sensor and cognitive radio networks, several multipath routing strategies have been proposed. An extensive survey of strategies for wireless sensor networks is given in Radi et al. (2012). There, protocols are divided into two groups: those designed to provide reliable data transmission and those designed to provide efficient resource utilization. Security is only mentioned in the context of one algorithm: H-SPREAD. In their seminal paper, Lou and Kwon (2006) show mathematically and empirically that both the security and reliability of a wireless sensor network can be improved through multipath routing. As a general rule, redundancy in transmitting data should be avoided (because it gives more opportunity for an attack), while greater redundancy improves reliability. In the H-SPREAD multipath routing algorithm secret sharing and multipath dispersion are combined to enhance security (a small number of individually compromised transmissions will not compromise the entire message), while discovering alternate paths at each node increases reliability.

Multipath routing and cryptographic solutions are not mutually exclusive. They can be used in conjunction to provide increased security. A multipath technique described in Bhattacharya et al. (2018) shuffles the bits of an original packet which are then sent across multiple paths. In this scheme it is "extremely difficult for an eavesdropper to guess any part of the original information from the sub-packets received along a single route as they contain only some selected bits of the original packet." (Bhattacharya et al. 2018) In addition, lightweight cipher algorithms exist that are specifically designed for energy and computational resource constrained devices in wireless networks (Maity et al. 2017; Katagi et al. 2008). The use of node-disjoint paths in addition to encryption to increase security is discussed in Alwan and Agarwal (2013).

Methodology

City section mobility model

We incorporate the movement of nodes by utilizing the City Section Mobility Model

proposed by Davies et al. (2000). The City Section Mobility Model imitates a city by restricting the movements of mobile nodes along coordinates representing streets, buildings and other city structures. It specifies a grid of "streets", and nodes are only able to move along streets and intersections. This mimics a city because people do not move through buildings and other structures. An example of construction along a grid is shown in Fig. 1. In the actual simulation, the area is represented by a 9000 by 12000 grid, where each unit represents one meter of distance. This data is based on the size of the city of Chicago, Illinois, USA. The grid represents horizontal and vertical streets within a city. Streets are placed 12 meters apart in the simulation area.

In the City Section Mobility Model, each node represents a mobile device in the city. Each device begins the simulation at a predefined intersection of two streets. The device then randomly chooses an intersection as a destination. During each iteration, each node picks a direction and moves towards the destination. After reaching the first destination, nodes randomly choose another destination which is also an intersection of two streets, and the process repeats. Each simulation was run for 1000 iterations. Numbers reported below are the average of 500 simulations.

Transmission radius and eavesdropping rate

In our simulation, nodes are able to communicate with other nodes within a communication range. We distinguish two nodes, the source node, where the message originates, and the destination node, where the message terminates. During the simulation we identify all relay nodes (except source and destination) as eavesdropping nodes. As is noted in Murakami et al. (2015), this situation in which almost all nodes are attack nodes "is an extremely hostile environment for networks."

The initial estimate for the transmission radius is 1000 meters, which was obtained from Mumtaz et al. (2014). During the simulation, we test three different transmission radii (500, 1000, and 1500 meters). By doing this, we are able to analyze how the radius impacts the connectivity of the graph and therefore an eavesdropper's ability to intercept a message.

The output of the simulation is an eavesdropping rate. We obtain this rate by counting the number of nodes that intercept the entire message along both paths and dividing by the total number of nodes in both paths. Using this ratio, we are able to determine the effectiveness of each algorithm in finding the least-interfered path.

Three algorithms for multipath routing

Our simulations compare three different algorithms. The first algorithm is our own, created by combining ideas from two algorithms in the literature. The other two are common, well-known algorithms, selected to show results when multipath routing is used, but the security aspects of choosing interference-aware paths are not taken into account. Simulations are executed as follows. Each algorithm selects two paths starting at a source node and terminating at a destination node. Three different interference radii were used: 500 meters, 1000 meters, and 1500 meters. We ran each of these radii with different node densities to simulate city areas of varying sizes. The number of mobile nodes in a simulation area varied between 5000, 10,000, and 15,000. Below we discuss the three algorithms.

1 *Least Interference Path*
The goal in this method is to find two paths that have the least interference, and are preferably interference-disjoint. This is based on ideas from Plummer et al. (2007) and also Le (2012), where edges are weighted according to interference levels. Le notes the importance and difficulty of finding interference-aware paths in polynomial time; calculations must occur quickly in a rapidly-changing network. In Le's algorithm, the network is considered as a weighted directed graph, where the weight of each edge is the "link interference level", and that level is determined by dividing the interference region of a link into smaller regions. In Plummer et al. a conflict graph (as described above in the "Disjoint paths, graph coloring and conflict graphs" section) is created to measure interference levels. In Le's case the paths are evaluated with Dijkstra's algorihtm, and in Plummer et al. the path is chosen adaptively at each node. In both Plummer et al. and Le, the resulting paths are evaluated in terms of network throughput only. Security aspects are not considered. We extend work on these ideas by evaluating results in terms of resistance to attacks. In our Least Interference Path algorithm, the first path is selected according to a redesign of Dijkstra's algorithm. In the simulation's connectivity graph, the degree of a node is determined by the number of other nodes within its transmission range. The degree represents the number of nodes capable of receiving a node's transmissions. A node with higher degree has greater potential to be eavesdropped on. In this graph, edge weights are assigned according to a node's degree. Edges with more potential eavesdroppers have a higher weight. When Dijkstra's shortest-paths algorithm is run on this graph, it picks the path with fewest potential eavesdropping neighbors. The nodes of the first path are removed from the graph, and a simple breadth-first search is used to find a second path. The time is therefore lower than running Dijkstra's algorithm twice. The algorithm results in a second path that is more direct than the first. This is desirable, because more direct paths speed transmissions. Also, maximally distant paths are not required, only interference disjoint paths. This algorithm is visualized in Fig. 2.
2 *Mock Suurballe's*
Thulasiraman, Chen and Shen mention using Suurballe's algorithm to find disjoint paths (Thulasiraman et al. 2011). Because Suurballe's algorithm requires negative directed edge weights, we are not able to use the exact version of it in our simulation. Suurballe's algorithm uses a version of Dijkstra's algorithm to find paths. Our Mock Suurballe's runs Dijkstra's algorithm twice on the graph. After the first run, the first path nodes are removed from the graph and the algorithm is run again. Suurballe's algorithm finds the two shortest disjoint paths in a network. The Mock Suurballe's algorithm finds two disjoint but relatively direct paths from the source to the destination. The method is visualized in Fig. 3.
3 *Random Direct Path*
The Random Direct Path method is run to give a baseline of performance when interference is not taken into account. It takes an idea from Plummer et al. (2007) in that the next hop of a path is chosen adaptively at each node. This method finds a path based on the distance of a node to the destination. The algorithm first discovers each neighbor node and then calculates the distance of those nodes to the destination node. It chooses the neighbor node with the shortest distance to the destination and

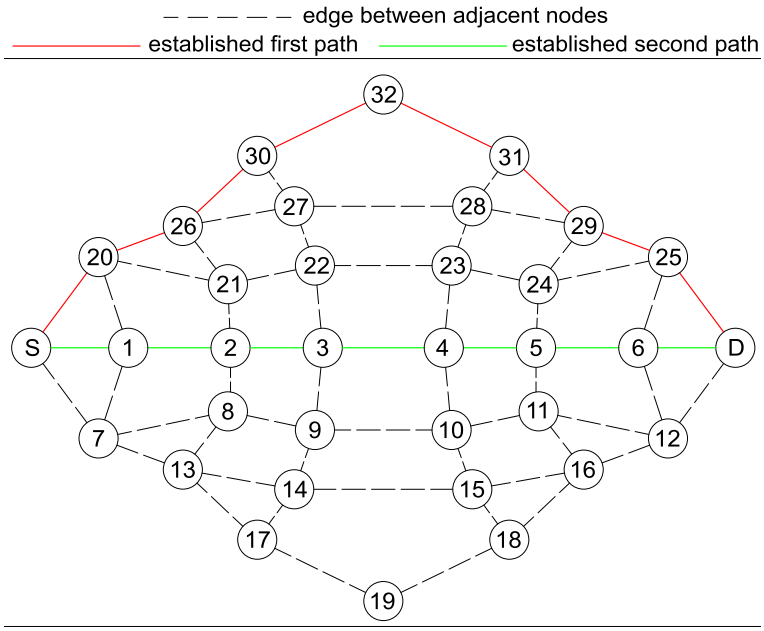

Fig. 2 Least Interefence Path Method. The first path, shown in red, is discovered by Dijkstra's algorithm based on a graph with interference-based weighted edges. The second path, shown in green, is discovered by a simple breadth-first search

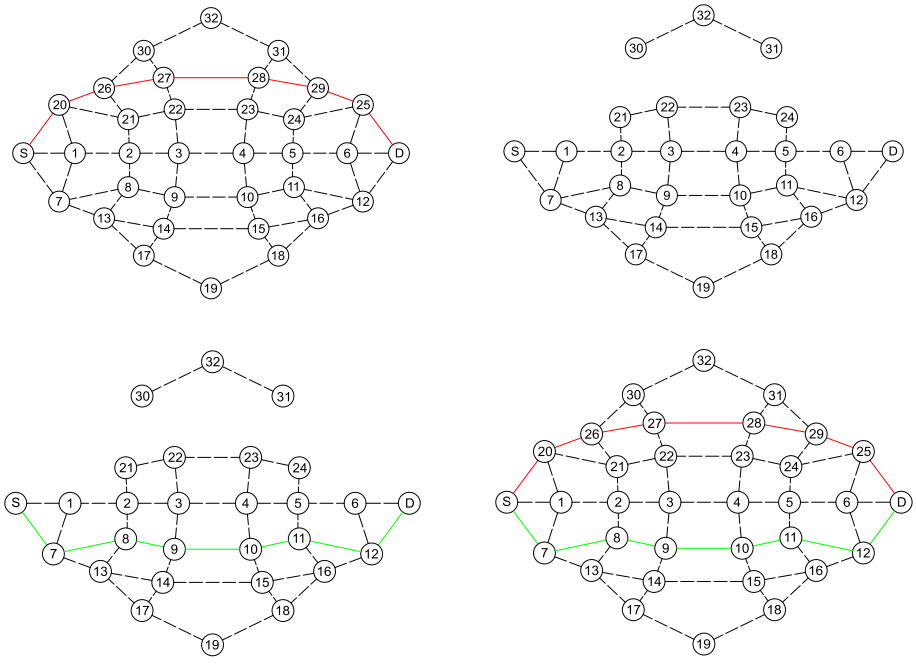

Fig. 3 Method 2 Mock Suurballe's. **a** Step 1. Dijkstra's algorithm is used to find a path from source to destination. **b** Step 2. Nodes in the first path are removed from the graph. **c** Step 3. A second path is chosen. **d** Step 4. Message is sent over two paths

then repeats the process. In this algorithm, our focus is solely on finding two paths. It is a low complexity method, provided for comparison with the first two methods. The method is visualized in Fig. 4.

Results

Table 1 shows the eavesdropping rates for each method with different radii and node densities in an extremely hostile environment in which every transmitting node is a malicious eavesdropper. The Least Interference Path algorithm has the lowest eavesdropping rate in every scenario, although there is no scenario in which eavesdropping is completely eliminated. In a large network with a large transmission radius, this algorithm results in a 28% eavesdropping rate, whereas with a smaller radius it results in an 11% rate. It is noted that, except in two cases (caused by the randomness of the experiment), the eavesdropping rate increases (or at least stays the same) as the radius increases. This indicates that the problem of eavesdropping will become increasingly pervasive as the practical transmission radius of mobile cellular devices increases. We also note that with the Least Interference Path method, the eavesdropping rate increases more slowly as the radius increases than with the other methods.

The Mock Suurballe's algorithm did only slightly better than the Random Direct Path algorithm. In both cases, interference-disjointness was not specifically enforced. The Random method had eavesdropping rates of approximately 50% under all conditions. This result is interesting for two reason. First, it reinforces our intuition that a higher density of nodes does not result in greater disjointedness if an algorithm does not seek it. On average, roughly the same number of hops were used for all densities, and the number

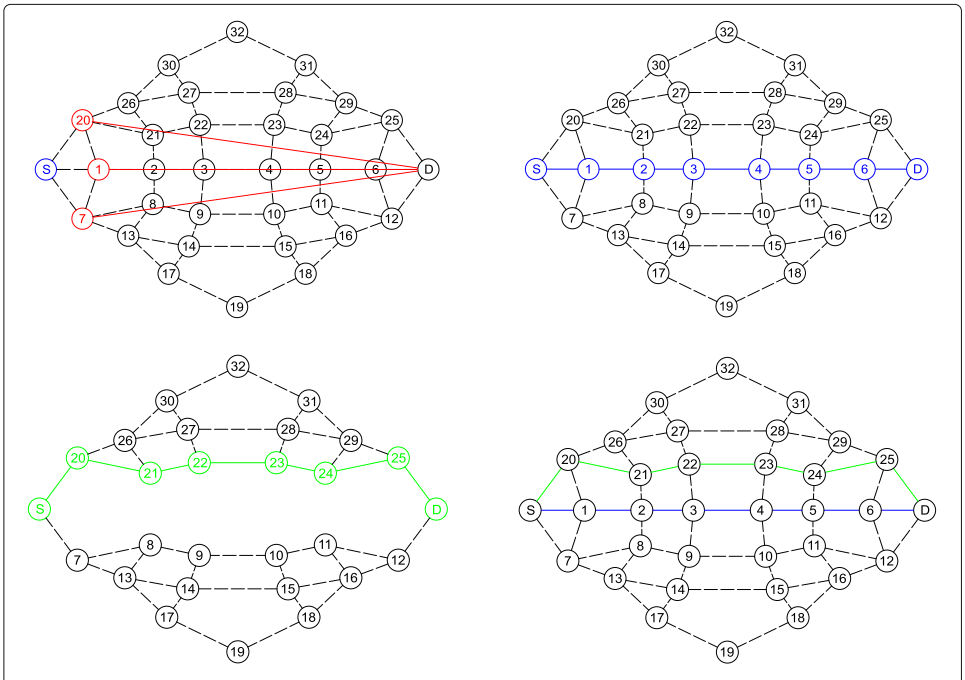

Fig. 4 Method 3 Random Direct Path. **a** Step 1. Nodes adjacent to the source node, shown in red, are evaluated according to their distance to the destination. **b** Step 2. A shortest-distance first path is chosen. **c** Step 3. The first path nodes are removed, and a second path is chosen using the methodology of step 1. **d** Step 4. Message is sent over two paths

Table 1 Results of three simulations

		Radius		
Algorithm		1500m	1000m	500m
Least Interference Path	5000 Nodes	0.31	0.24	0.12
	10,000 Nodes	0.19	0.34	0.19
	15,000 Nodes	0.28	0.15	0.11
Mock Suurballe's	5000 Nodes	0.46	0.44	0.38
	10,000 Nodes	0.42	0.41	0.29
	15,000 Nodes	0.45	0.43	0.40
Random Direct Path	5000 Nodes	0.49	0.49	0.49
	10,000 Nodes	0.49	0.50	0.48
	15,000 Nodes	0.50	0.50	0.49

Numbers show eavesdropping rates (average of 500 runs), which are the percentage of nodes that are successful eavesdroppers

of interference-disjoint nodes chosen was approximately the same. Second, it suggests that using multiple paths, even if only for purposes such as load balancing, has a security advantage and reduces possible eavesdroppers. Mock Suurballe's had a best result of 29%, approximately the same as the worst result under Least Interference Path.

As the number of nodes increases, it might be expected that the interference increases because of the density of the network. Interestingly, in our simulations an increase in node density did not generally cause the eavesdropping rate to increase. It seems that with a higher node density, there is a large corresponding increase in the number of possible paths. Therefore the algorithms were better able to find paths that did not interfere with one another.

Conclusion

Security is an important consideration in 5G networks, and many methods have been proposed to enhance it. It is interesting to observe that these methods differ from defenses against similar attacks on wired and other networks because of the unique properties of wireless and 5G networks.

Eavesdropping will be a constant problem due to open architecture and the cooperation of devices. Defenses range from simply moving away from the eavesdropper, to using friendly jamming to confuse it. Jamming limits the access of users to limited bandwidth resources. Again movement is a suggested defense, however this time it is the movement of the transmission to different channels, hopefully in a pattern that a jammer will be unable to detect. The primary user emulation attack is a form of denial-of-service attack to which 5G networks are particularly susceptible. Defenses against this type of attack involve determining the location of primary users in order to distinguish them from emulators. This can be done individually, through a dedicated sensor network, or through a group of devices using a non-centralized strategy. Last is the injecting attack, against which cryptography and authentication are often mentioned as defenses.

We have presented a comprehensive survey of the literature on these four types of attacks. In response to eavesdropping specifically, we have considered the defense strategy of multipath routing and the security implications related to it. Related works on multipath routing were presented, along with a simulation that tested three different methods of choosing the paths. It was found that strategies that choose interference-disjoint paths

work best to prevent eavesdropping. It was also found that, while increasing the broadcast radius of mobile devices increases potential eavesdropping, increasing the density of nodes mitigates the problem by providing additional possible paths.

Abbreviations

(RI^3M): Routing with Interflow and Intraflow Interference Metric; ACK: Acknowledgement; CIA: Confidentiality, Integrity and Authentication; CoSAP: Cognitive Spectrum Allocation Protocol; CRN: Cognitive Radio Network; CSC: Channel Switching Cost; D2D: Device-to-Device; DNDR: Dual Node-Disjoint Paths Routing; DoS: Denial of Service; FCC: Federal Communications Commission; FDM: Frequency Division Multiplexing; GCDCA: Graph Coloring based Dynamic Channel Allocation; IDS: Intrusion Detection System; IoT: Internet of Things; LBT: Listen Before Talk; maMIMO: Massive Multiple Input Multiple Output; MDP: Markov Decision Process; MIMO: Multiple Input Multiple Output; MLB: Multi-Armed Bandit; NCA: DeceNtralized Cooperative Anaylsis; NWAUF: Normalized Weighted Additive Utility Function; PC: Power Control; PKTH: Private Key Based Time Hopping; PLS: Physical Layer Security; PSK: Phase-Shift Keying; PU: Primary User; PUEA: Primary User Emulation Attack; QoS: Quality of Service; RFID: Radio Frequency Identification; SDTH: Selective Diversity Based Time Hopping; SDTP: Secure Data Transmission Protocol; SecMR: Secure Multipath Discovery Algorithm; SINR: Signal-to-Interference-Plus-Noise Ratio; SU: Secondary User; TDD: Time-Division Duplex; TDM: Time Division Multiplexing; UFH: Uncoordinated Frequency Hopping

Authors' contributions

All authors contributed to the survey section and participated in the writing. JT wrote the simulation software and is co-first-author of this paper. AC created all illustrations is co-first-author of this paper. JM supervised the writing and is corresponding author. All authors read and approved the final manuscript.

Funding

No funding was allocated for this work.

Availability of data and materials

The software created for this paper is available from the corresponding author on reasonable request.

Competing interests

The authors declare that they have no competing interests.

Author details

[1] Southern Illinois University Edwardsville, Edwardsville, IL, USA. [2] Southern Illinois University Carbondale, Carbondale, IL, USA.

Received: 29 April 2019 Accepted: 2 October 2019
Published online: 08 November 2019

References

Abualhaol I, Muegge S (2016) Securing d2d wireless links by continuous authenticity with legitimacy patterns. In: 2016 49th Hawaii International Conference on System Sciences (HICSS). pp 5763–5771. https://doi.org/10.1109/HICSS.2016.713

Adem N, Hamdaoui B, Yavuz A (2015) Pseudorandom time-hopping anti-jamming technique for mobile cognitive users. In: 2015 IEEE Globecom Workshops (GC Wkshps). pp 1–6. https://doi.org/10.1109/GLOCOMW.2015.7414043

Adem N, Hamdaoui B, Yavuz A (2016) Mitigating jamming attacks in mobile cognitive networks through time hopping. Wirel Commun Mobile Comput. https://doi.org/10.1002/wcm.2745

AlDairi A, et al. (2017) Cyber security attacks on smart cities and associated mobile technologies. Procedia Comput Sci 109:1086–1091

Alavi F, Yamchi NM, Javan MR, Cumanan K (2017) Limited feedback scheme for device-to-device communications in 5g cellular networks with reliability and cellular secrecy outage constraints. IEEE Trans Veh Technol 66(9):8072–8085

Alwan H, Agarwal A (2013) A multipath routing approach for secure and reliable data delivery in wireless sensor networks. Int J Distrib Sens Netw 9(3):232798

Bhattacharya A, Audhya S, Sinha K (2016) An anti-jamming protocol based on secret reallocation of channels. In: 2016 3rd International Conference on Recent Advances in Information Technology (RAIT). pp 154–159. https://doi.org/10.1109/RAIT.2016.7507893

Bhattacharya A, Ghosh SC, Sinha K, Sinha BP (2018) Secure multipath routing for multimedia communication in cognitive radio networks. Int J Commun Netw Distrib Syst 21(1):26–55

Ben-Othman J, Yahya B (2010) Energy efficient and qos based routing protocol for wireless sensor networks. J Parallel Distrib Comput 70(8):849–857

Borges P, Sousa B, Ferreira L, Saghezchi FB, Mantas G, Ribeiro J, Rodriguez J, Cordeiro L, Simoes P (2017) Towards a hybrid intrusion detection system for android-based ppdr terminals. In: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). IEEE. pp 1034–1039. https://doi.org/10.23919/inm.2017.7987434

Chen R, Park JM (2006) Ensuring trustworthy spectrum sensing in cognitive radio networks. In: Networking Technologies for Software Defined Radio Networks, 2006. SDR '06.1st IEEE Workshop On. pp 110–119. https://doi.org/10.1109/SDR.2006.4286333

Chen R, Park JM, Reed JH (2008) Defense against primary user emulation attacks in cognitive radio networks. IEEE J Sel Areas Commun 26(1):25–37. https://doi.org/10.1109/JSAC.2008.080104

Cikovskis L, Slaidins I (2015) Path selection criteria for multi-path routing in wireless ad-hoc network. In: 2015 Advances in Wireless and Optical Communications (RTUWO). pp 58–61. https://doi.org/10.1109/RTUWO.2015.7365720

Cumanan K, Xing H, Xu P, Zheng G, Dai X, Nallanathan A, Ding Z, Karagiannidis GK (2017) Physical layer security jamming: Theoretical limits and practical designs in wireless networks. IEEE Access 5:3603–3611
Das D, Das S (2013) Primary user emulation attack in cognitive radio networks: A survey. IRACST-International Journal of Computer Networks and Wireless Communications 3(3):312–318
Davies VA, et al. (2000) Evaluating mobility models within an ad hoc network. Master's thesis, Citeseer
Eisenbarth T, Kumar S, Paar C, Poschmann A, Uhsadel L (2007) A survey of lightweight-cryptography implementations. IEEE Des Test Comput 24(6):522–533
Faisal M, Mathkoor H (2015) Sdtp: Secure data transmission protocol in ad hoc networks based on link-disjoint multipath routing. In: 2015 2nd World Symposium on Web Applications and Networking (WSWAN). pp 1–5. https://doi.org/10.1109/WSWAN.2015.7210348
Fang D, Qian Y, Hu RQ (2018) Security for 5g mobile wireless networks. IEEE Access 6:4850–4874
Fauzi A, Khan A (2017) Threats advancement in primary user emulation attack and spectrum sensing data falsification (ssdf) attack in cognitive radio network (crn) for 5g wireless network environment. J Telecommun Electron Comput Eng (JTEC) 9(2-10):179–183
Ganjali Y, Keshavarzian A (2004) Load balancing in ad hoc networks: single-path routing vs. multi-path routing. In: IEEE INFOCOM 2004. IEEE Vol. 2. pp 1120–1125. https://doi.org/10.1109/infcom.2004.1356998
Ge X, Cheng H, Guizani M, Han T (2014) 5g wireless backhaul networks: challenges and research advance. arXiv preprint arXiv:1412.7232
Gharaibeh A, Salahuddin MA, Hussini SJ, Khreishah A, Khalil I, Guizani M, Al-Fuqaha A (2017) Smart cities: A survey on data management, security, and enabling technologies. IEEE Commun Surv Tutor 19(4):2456–2501
Huifang C, Lei X, Xiong N (2014) Reputation-based hierarchically cooperative spectrum sensing scheme in cognitive radio networks. China Commun 11(1):12–25. https://doi.org/10.1109/CC.2014.6821304
Huo Y, Tian Y, Ma L, Cheng X, Jing T (2018) Jamming strategies for physical layer security. IEEE Wirel Commun 25(1):148–153
Jameel F, Wyne S, Kaddoum G, Duong TQ (2018) A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. IEEE Commun Surv Tutor 21(3):2734–2771. https://doi.org/10.1109/comst.2018.2865607
Jiang F, Zhu C, Peng J, Liu W, Zhu Z, He Y (2015) Joint relay and jammer selection and power control for physical layer security in two-way relay networks with imperfect csi. Wirel Pers Commun 85(3):841–862
Jin Z, Anand S, Subbalakshmi KP (2010) Robust spectrum decision protocol against primary user emulation attacks in dynamic spectrum access networks. In: Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE. pp 1–5. https://doi.org/10.1109/GLOCOM.2010.5683174
Jin Z, Anand S, Subbalakshmi KP, Chandramouli R (2016) Connectivity of ad hoc 5g wireless networks under denial of service attacks. River Publishers. 5G Outlook-Innovations and Applications
Kapetanovic D, Zheng G, Rusek F (2015) Physical layer security for massive mimo: An overview on passive eavesdropping and active attacks. IEEE Commun Mag 53(6):21–27
Katagi M, Moriai S, et al. (2008) Lightweight cryptography for the internet of things. Sony Corporation: 7–10
Khan A, Javed Y, Abdullah J, Nazim J, Khan N (2017) Security issues in 5g device to device communication. IJCSNS 17(5):366
Kuperman G, Modiano E (2014) Disjoint path protection in multi-hop wireless networks with interference constraints. In: 2014 IEEE Global Communications Conference. pp 4472–4477. https://doi.org/10.1109/GLOCOM.2014.7037512
Le PH (2012) A performance evaluation of multi-path routing protocols for mobile ad hoc networks. In: 2012 IEEE 15th International Conference on Computational Science and Engineering. pp 484–491. https://doi.org/10.1109/ICCSE.2012.73
Li X, Cadeau W (2011) Anti-jamming performance of cognitive radio networks. In: Information Sciences and Systems (CISS), 2011 45th Annual Conference On. pp 1–6. https://doi.org/10.1109/CISS.2011.5766199
Lichtman M, Rao R, Marojevic V, Reed J, Jover RP (2018) 5g nr jamming, spoofing, and sniffing: threat assessment and mitigation. In: 2018 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE. pp 1–6. https://doi.org/10.1109/iccw.2018.8403769
Lou W, Kwon Y (2006) H-spread: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks. IEEE Trans Veh Technol 55(4):1320–1330
Maity S, Sinha K, Sinha BP (2017) An efficient lightweight stream cipher algorithm for wireless networks. In: 2017 IEEE Wireless Communications and Networking Conference (WCNC). IEEE. pp 1–6. https://doi.org/10.1109/wcnc.2017.7925562
Mavropodi R, Kotzanikolaou P, Douligeris C (2007) Secmr – a secure multipath routing protocol for ad hoc networks. Ad Hoc Networks 5(1):87–99. https://doi.org/10.1016/j.adhoc.2006.05.020. Security Issues in Sensor and Ad Hoc Networks
McGarry T Federal Communications Commission Technological Advisory Council, 5G Cybersecurity Subcommittee. Available at https://www.fcc.gov/general/tac-reportsand-papers. Accessed 9 Dec 2016
Mucchi L, Ronga L, Huang K, Chen Y, Wang R (2017) A new physical-layer security measure-secrecy pressure. In: GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE. pp 1–6. https://doi.org/10.1109/glocom.2017.8254006
Mumtaz S, Huq KMS, Rodriguez J (2014) Direct mobile-to-mobile communication: Paradigm for 5g. IEEE Wirel Commun 21(5):14–23
Munir A, Qian Z, Shafiq Z, Liu A, Le F (2017) Multipath tcp traffic diversion attacks and countermeasures. In: 2017 IEEE 25th International Conference on Network Protocols (ICNP). IEEE. pp 1–10. https://doi.org/10.1109/icnp.2017.8117547
Murakami T, Kimura T, Uemori T, Kohno E, Kakuda Y (2015) On notification message re-broadcasting for the node-disjoint multipath routing method in ad hoc networks to counter eavesdropping of data packets. In: 2015 IEEE 35th International Conference on Distributed Computing Systems Workshops. pp 11–16. https://doi.org/10.1109/ICDCSW.2015.14
Naqvi B, Rashid I, Riaz F, Aslam B (2013) Primary user emulation attack and their mitigation strategies: A survey. In: Information Assurance (NCIA), 2013 2nd National Conference On. pp 95–100. https://doi.org/10.1109/NCIA.2013.6725331

Naslund M, Phillips S, Surridge M, Moraru M, Heikkinen S, Pernila T, Arfaoui G, Sanchez Vilchez JM, Wary J-P, O'Hanlon P, et al. (2016) 5g-ensure-d2. 3 risk assessment, mitigationReferences: Citation details for references [Naslund et al. (2016); Jin et al. (2016); Pedhadiya et al. (2018); Wang et al. (2001)] are incomplete. Please supply the "Publisher address" of these references. Otherwise, kindly advise us on how to proceed. and requirements (draft). ALBLF and 5G-ENSURE Consortium

Orsino A, Araniti G, Militano L, Alonso-Zarate J, Molinaro A, Iera A (2016) Energy efficient iot data collection in smart cities exploiting d2d communications. Sensors 16(6):836

Pearlman MR, Haas ZJ, Sholander P, Tabrizi SS (2000) On the impact of alternate path routing for load balancing in mobile ad hoc networks. In: 2000 First Annual Workshop on Mobile and Ad Hoc Networking and Computing. MobiHOC (Cat. No. 00EX444). IEEE. pp 3–10. https://doi.org/10.1109/mobhoc.2000.869207

Pedhadiya MK, Jha RK, Bhatt HG (2018) Device to device communication: A survey. Elsevier. Journal of Network and Computer Applications

Plummer A, Wu T, Biswas S (2007) A cognitive spectrum assignment protocol using distributed conflict graph construction. In: MILCOM 2007 - IEEE Military Communications Conference. pp 1–7. https://doi.org/10.1109/MILCOM.2007.4455299

Porambage P, Ylianttila M, Schmitt C, Kumar P, Gurtov A, Vasilakos AV (2016) The quest for privacy in the internet of things. IEEE Cloud Comput 3(2):36–45. https://doi.org/10.1109/MCC.2016.28

Radi M, Dezfouli B, Bakar KA, Lee M (2012) Multipath routing in wireless sensor networks: survey and research challenges. Sensors 12(1):650–685

Safdar GA, Ur-Rehman M, Muhammad M, Imran MA, Tafazolli R (2016) Interference mitigation in d2d communication underlaying lte-a network. IEEE Access PP(99):1–1. https://doi.org/10.1109/ACCESS.2016.2621115

Sarma S, Kuri J (2015) Optimal power allocation for protective jamming in wireless networks. Comput Netw 81(C):258–271. https://doi.org/10.1016/j.comnet.2015.02.011

Schneider P, Horn G (2015) Towards 5G Security. In: 2015 IEEE Trustcom/BigDataSE/ISPA. Helsinki. pp 1165–1170. https://doi.org/10.1109/Trustcom.2015.499

Sedidi R, Kumar A (2016) Key exchange protocols for secure device-to-device (d2d) communication in 5g. In: 2016 Wireless Days (WD). pp 1–6. https://doi.org/10.1109/WD.2016.7461477

Shafiq MZ, Le F, Srivatsa M, Liu AX (2013) Cross-path inference attacks on multipath tcp. In: Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks–HotNets-XII. ACM. p 15. https://doi.org/10.1145/2535771.2535782

Skouby KE, Lynggaard P (2014) Smart home and smart city solutions enabled by 5g, iot, aai and cot services. In: 2014 International Conference on Contemporary Computing and Informatics (IC3I). IEEE. pp 874–878. https://doi.org/10.1109/ic3i.2014.7019822

Soto J, Queiroz S, Gregori M, Nogueira M (2013) A flexible multi-criteria scheme to detect primary user emulation attacks in crahns. In: World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on A. pp 1–6. https://doi.org/10.1109/WoWMoM.2013.6583453

Strasser M, Pöpper C, Capkun S, Cagalj M (2008) Jamming-resistant key establishment using uncoordinated frequency hopping. In: 2008 IEEE Symposium on Security and Privacy (sp 2008). pp 64–78. https://doi.org/10.1109/SP.2008.9

Su H, Wang Q, Ren K, Xing K (2011) Jamming-resilient dynamic spectrum access for cognitive radio networks. In: 2011 IEEE International Conference on Communications (ICC). IEEE. pp 1–5. https://doi.org/10.1109/icc.2011.5962525

Sun L, Du Q (2017) Physical layer security with its applications in 5g networks: A review. China Commun 14(12):1–14

Teotia V, Kumar V, Minz S (2015) Conflict graph based channel allocation in cognitive radio networks. In: 2015 IEEE 34th Symposium on Reliable Distributed Systems Workshop (SRDSW). pp 52–56. https://doi.org/10.1109/SRDSW.2015.19

Thulasiraman P, Chen J, Shen X (2011) Multipath routing and max-min fair qos provisioning under interference constraints in wireless multihop networks. IEEE Transactions on Parallel and Distributed Systems 22(5):716–728. https://doi.org/10.1109/TPDS.2010.145

Tran D. A., Raghavendra H. (2005) Routing with congestion awareness and adaptivity in mobile ad hoc networks. In: IEEE Wireless Communications and Networking Conference, 2005. IEEE Vol. 4. pp 1988–1994. https://doi.org/10.1109/wcnc.2005.1424824

Tushir B, Dhurandher SK, Woungang I, Obaidat MS, Teotia V (2016) Graph colouring technique for efficient channel allocation in cognitive radio networks. In: 2016 IEEE International Conference on Communications (ICC). pp 1–5. https://doi.org/10.1109/ICC.2016.7510607

Velásquez-Villada C, Donoso Y (2013) Multipath routing network management protocol for resilient and energy efficient wireless sensor networks. Procedia Comput Sci 17:387–394

Wang L, Shu Y, Dong M, Zhang L, Yang OW (2001) Adaptive multipath source routing in ad hoc networks. In: ICC 2001. IEEE International Conference on Communications. Conference Record (Cat. No. 01CH37240). IEEE Vol. 3. pp 867–871

Wang M, Yan Z (2015) Security in d2d communications: A review. In: Trustcom/BigDataSE/ISPA, 2015 IEEE Vol. 1. pp 1199–1204. https://doi.org/10.1109/Trustcom.2015.505

Wu Y, Wang B, Liu KJR, Clancy TC (2012) Anti-jamming games in multi-channel cognitive radio networks. IEEE Journal on Selected Areas in Communications 30(1):4–15. https://doi.org/10.1109/JSAC.2012.120102

Wu W, Zhang Y (2014) Constructing conflict graph for d2d communications in cellular systems. In: 2014 Sixth International Conference on Wireless Communications and Signal Processing (WCSP). pp 1–6. https://doi.org/10.1109/WCSP.2014.6992092

Yang Y, Wang J, Kravets R (2005) Designing routing metrics for mesh networks. In: IEEE Workshop on Wireless Mesh Networks (WiMesh), Santa Clara. pp 1–9

Yang S, Tang W (2014) On the maximum throughput of multiple-path transmission via irreducible and neighbor-disjoint paths in multiple-hop wireless networks. In: 2014 European Modelling Symposium. pp 397–402. https://doi.org/10.1109/EMS.2014.42

Yang F, Wang Q, Amer PD (2014) Out-of-order transmission for in-order arrival scheduling for multipath tcp. In: 2014 28th International Conference on Advanced Information Networking and Applications Workshops. IEEE. pp 749–752. https://doi.org/10.1109/waina.2014.122

Yang N, Wang L, Geraci G, Elkashlan M, Yuan J, Di Renzo M (2015) Safeguarding 5g wireless communication networks using physical layer security. IEEE Commun Mag 53(4):20–27
Yu Y, Liang M (2015) A node-disjoint multipath routing protocol in manets. In: 2015 International Conference on Computer Science and Mechanical Automation (CSMA). pp 108–112. https://doi.org/10.1109/CSMA.2015.28
Yu T, Jin H, Nahrstedt K (2016) Writinghacker: Audio based eavesdropping of handwriting via mobile devices. In: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing, UbiComp '16. ACM, New York. pp 463–473. https://doi.org/10.1145/2971648.2971681. http://doi.acm.org.libproxy.siue.edu/10.1145/2971648.2971681
Xie N, Zhang S (2018) Blind authentication at the physical layer under time-varying fading channels. IEEE J Sel Areas Commun 36(7):1465–1479
Xu Y, Liu Y, Yang K, Li D, Labs QLB (2013) Interference mitigation scheme for device-to-device communication with qos constraint. In: 2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). pp 1784–1788. https://doi.org/10.1109/PIMRC.2013.6666432
Xu J, Duan L, Zhang R (2017) Proactive eavesdropping via cognitive jamming in fading channels. IEEE Trans Wirel Commun 16(5):2790–2806
Xu J, Duan L, Zhang R (2017) Surveillance and intervention of infrastructure-free mobile communications: A new wireless security paradigm. IEEE Wirel Commun 24(4):152–159
Zhang R, Song L, Han Z, Jiao B, Debbah M (2010) Physical layer security for two way relay communications with friendly jammers. In: Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE. pp 1–6. https://doi.org/10.1109/GLOCOM.2010.5683465
Zou Y, Zhu J, Wang X, Hanzo L (2016) A survey on wireless security: Technical challenges, recent advances, and future trends. Proceedings of the IEEE 104(9):1727–1765. https://doi.org/10.1109/jproc.2016.2558521

Publisher's Note