International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2019): 7.583

Prevent the Eavesdropping in D2D Networks by Using Network Coding and Signal-To-Noise (SNR)

Yousef Ali Alshami[1], Shiv Kumar[2]

[1]Pursuing master's degree program in Information Security in Mewar University, Chittorgarh, Rajasthan, India
Email: *eng.yousufalshami[at]gmail.com*

[2]Assistant Professor in Mewar University, Chittorgarh, Rajasthan, India
Email: *shivkumar004[at]gmail.com*

Abstract: ***Due to the transmission idea of remote device-to-device organizations, the transmission of private data is undermined by the outside listening in. Focusing on this issue, we together adventure Wyner's code and the straight organization coding, in this paper, to improve the security. The capacity of Wyner's code requires the authentic channel in a way that is better than the busybody's channel, so we propose a novel hand-off determination plan to accomplish this target. In particular, two gatherings of transfers have been chosen. Re-lays in one of the gatherings are chosen to advance the private data, and transfers in the other gathering are chosen to send arti-facial noise. Along these lines, we ensure that the signal-to-noise ratio (SNR) at the authentic recipient is bigger than an objective worth however the SNR at the busybody has a specific likelihood not exactly the objective worth so the security can be upgraded. Also, zeroing in on the issue that Wyner's code can't accomplish security if the SNR at the snoop is bigger than the objective worth, we propose an organization coding strategy. In this technique, the message to be communicated is partitioned into different parts, and afterward, these parts are associated with one another by utilizing network coding. In this manner, the busybody likewise can't unravel the private in-arrangement even its SNR bigger than the objective worth. We break down the mystery blackout likelihood in principle, and the reproduction results are given to affirm our investigation.***

Keywords: eavesdroppers, D2D, relay selection, signal-to-noise rate, heterogeneous

1. Introduction

Remote Device-to-device (D2D) correspondences empower the devices with a short-range in the cell organization to impart straightforwardly, which improves the effectiveness of unearthly usage and asset planning [1],[2]. In any case, due to the naturally broadcast nature of remote interchanges, the private data communicated by D2D devices is defenseless against snooping. To address this issue, and arising technique called physical-layer security has been broadly concentrated as of late [3]. Unique in relation to the customary encryption-based strategies, physical-layer security can accomplish keyless mystery by utilizing Wyner's code [4] if the authentic channel is superior to the busybody's channel. Spurred by this edify ing result, an enormous number of works plan to improve security by upgrading the genuine channel or/and debasing the snoop's channel. Among these works, one of the significant branches is the investigation of helpful correspondences. Agreeable correspondence was initially utilized to stretch out the transmission range and to improve dependability.

As of late, it is utilized to improve security. In agreeable correspondence, there are by and large two jobs for a hand-off or a partner hub to help the safe transmission: forward the data or send fake noise. In particular, when sending the private data, intensified and-forward (AF) and decipher and-forward (DF) are the most widely recognized protocols. When there are numerous transfers in the organization, hand-off choice is an effective method to improve security. In [5], Feng et al. consider a multiuser and multi-transfer organization and select the best client and the best hand-off to amplify the got signal-to-obstruction to-noise ratio (SINR). Support helped transfer choice plan is proposed, and the creators break down the compromise between the security and the postponement. In [6] transfer choice is utilized in the enormous scope of MIMO frameworks, and force distribution is utilized to additional upgrade the security. transfer determination is utilized to improve both the security and the unwavering quality of psychological radio frameworks. In these works, a typical character is that the immediate connection between the transmitter and the authentic recipient doesn't exist. Notwithstanding, for D2D interchanges, the immediate connection is likely in present, so it ought to be considered.

Thinking about this issue, a deft transfer determination conspire is proposed in their works, the hand-off which can disentangle the private data from the transmitter and has the best channel to the authentic recipient is chosen to advance the private data. In any case, by and by, if the goal is to choose the best hand-off, each transfer should share the information about the channel side data (CSI) to different transfers. Clearly, this will be mind-boggling and wasteful if there are various transfers in the organization. Also, all the works examined above don't consider the circumstance after the mystery blackout happens when utilizing Wyner's code. This shows that the busybody can unravel the private data straightforwardly in the event that it has a superior channel quality.

1.1. Eavesdropping

1.1.1. Definition of Eavesdropping attack

Eavesdropping assault, otherwise called sniffing or sneaking around assault, happens when an unapproved party takes,

modifies, or erases fundamental data that is sent between two electronic devices.

Here's a model

A distant representative associate over an open organization and sends across some essential business data to his colalliance. The data is being communicated over the open organization, and the digital assailant quietly interrupts all the data on the organization's traffic. Presently, to forestall an Eavesdropping assault, the representative may decide to connect over a Virtual Private Network, which is moderately more secure than an open organization. Yet, this again is definitely not a full-evidence strategy (particularly in the event that you don't have the foggiest idea how secure is your VPN) to battle eavesdropping assault; the assailant puts a bit of programming or organization sniffers in the net-work pathway that will monitor, record and accumulate all the basic business data.

As Tom King, applications and security chief at 3i, composes Eavesdropping assaults are guileful in light of the fact that it's hard to realize they are happening. When associated with an organization, clients may accidentally take care of delicate information — passwords, account numbers, riding propensities, the substance of email messages — to an assailant.

We should now comprehend the various situations that aggressors influence on for a vindictive Eavesdropping at-tack.

1) Weak Passwords: by picking frail passwords, that can be undermined effectively, you are leaving the entryway to a classified correspondence channel totally open. When the assailant has your secret phrase, he can without much of a stretch join the organization on which important business data is being exchanged.
2) Working distantly: representatives working in the office premises adjust to the security principles and are associated with a protected organization. However, distant workers may interface their devices to a powerless or unreliable organization that could be inclined to an eavesdropping assault
3) Frail organizations: interfacing with open organizations that don't need passwords for access and communicates data without encryption is an ideal set up for an aggressor to convey a snoop ping assault.

1.2. Network Coding

1.2.1. Definition of Network Coding

Network coding is a networking strategy where operations, which by and by will, in general, be mathematical calculations, are performed on information as it goes through the hubs inside a network. While in principle any way of the calculation could be performed on the information at a hub, current NC calculations will in general be worried about aggregating the different transmissions that go through a given hub. In customary directing networks, bundles are essentially stored and afterward sent to the following hub downstream in the network. In that capacity, if a directing hub gets two bundles from two particular sources it will advance them consecutively, regardless of whether they are both routed to a similar objective while queueing any others it might get meanwhile. This outcome in the hub making separate transmissions for every single message being conveyed, which brings about abatement in network effectiveness. NC is utilized to moderate this by consolidating applicable messages at the hand-off hub, utilizing a given encoding, at that point sending this gathered outcome to the objective for decoding. With the goal for everything to fall into place, the objective hub should be synchronized with the communicating hubs, an imperative particularly significant with regards to network coding done at the actual layer.

1.2.1.1. Network coding in D2D

Here we think about the cases without a base station. All interchanges include exclusively devices and not the base station. The base station could be utilized to build up D2D correspondence. We detail the situations where network coding could be utilized with D2D Net-work.

1.2.2.1. Multiple Unicast

D2D correspondence with numerous unicast streams happens when more than one device needs to send and they exceptionally close, they can arrive at one another utilizing direct correspondence or multihop. This is where two individuals utilizing mobile phones are talking or sending multimedia to one another, and they are reachable from one another in a D2D network. Figure 6 portrays the addition of network coding in D2D correspondence with products unicasts. In conventional directing without network coding, the halfway steering device needs to advance each bundle. With network coding, the middle defeating device can consolidate the messages it got and communicate one network coding message by means of transmission, saving assets, and lessening the general inactivity. In the model with two devices, network coding saved one message. The more devices that are in a similar locale, the more prominent the addition of network coding. In numerous unicast, thinking about no bundle misfortune, with n devices, in non-coding steering 2n messages are important. With network coding, the primary n messages are typically communicated, and the halfway steering device produces one network coding message, diminishing the total number of messages to n + 1. With parcel misfortunes, the upside of utilizing network coding increments.

1.2.2. Multicast

In D2D multicast streams, more than one device needs to get similar data from a close-by device. This is the situation, for instance, when more than one for each child is sharing a video. This is likewise the situation when there is an occasion for some individuals with a similar interest, and no foundation base station is accessible, for example, in an impromptu crisis salvage. One can see that, in D2D correspondence utilizing multicast, the total number of messages sent is additionally diminished. In customary multicast, the devices need to advance each parcel. With network coding, the devices can join messages and send a network coding message. The receiver translates utilizing the recently got messages. For instance, if a device gets message An and later A XOR B, it can disentangle B by doing A XOR (A XOR B). The equivalent should be possible utilizing direct coding or irregular straight coding portrayed before in the paper. This again saves assets important in 5G and D2D communications, including data transmission, channel usage, energy,

and furthermore lessens the general idleness. For the case with two messages, the general dormancy decreased from four-time allotments to three. The more devices there are, the more prominent the advantages of network coding in multicast.

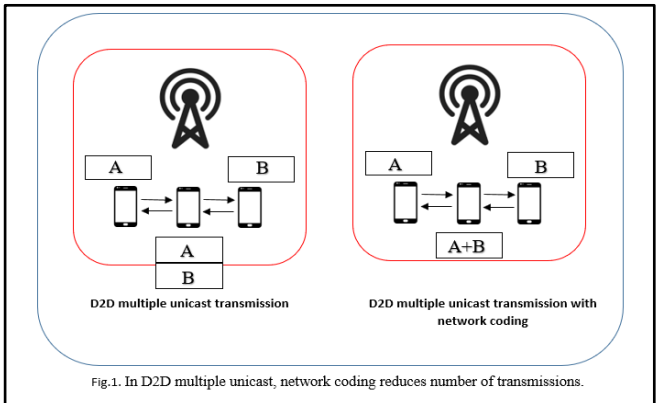

Fig.1. In D2D multiple unicast, network coding reduces number of transmissions.

1.3. Signal to Noise Ratio (SNR)

As a teenager, while learning the ins and outs of car audio, I often basked in the sheer detail of every note. For me, music was intoxicating, almost as much as the fields of Science and Electronics. However, during this time, the onset of the compact disc and, of course, the car subwoofer was taking center stage.

1.3.1. Definition of Signal to Noise Ratio

Regarding definition, SNR or signal-to-noise ratio is the ratio between the ideal data or the intensity of a signal and the undesired signal or the intensity of the foundation noise. Additionally, SNR is an estimation boundary being used in the fields of science and designing that looks at the degree of the ideal signal to the degree of foundation noise. All in all, SNR is the ratio of signal capacity to the noise force, and its unit of articulation is regularly decibels (dB). Additionally, a ratio more noteworthy than 0 dB or higher than 1:1, means more signal than noise.

Besides the specialized meaning of SNR, the manner in which I characterize it in different terms is by utilizing a near. For instance, say that you and one other individual are inside a huge room having a discussion. Nonetheless, the room is brimming with others who are likewise having conversations. Moreover, a couple of the others additionally have comparable voice examples to you and different individuals engaged with your conversation. As you can envision, it is hard to unravel which individual is stating what.

1.3.2 The Basics of Signal to Noise Ratio Calculations

In fundamental terms, SNR is the distinction between the ideal signal and the noise floor. Likewise, as far as definition, the noise floor is the presumptive foundation transmissions that are created by different devices or by devices that are accidentally producing interference on a comparable recurrence. Thusly, to discover the signal to noise ratio, one should locate the quantifiable difference between the ideal signal strength and the undesirable noise by taking away the noise an incentive from the signal strength esteem.

Speculatively talking, if your device's radio gets a signal at -65 dBm (decibels per milliwatt), and the noise floor is - 80 dBm, at that point the subsequent signal to noise ratio is 15 dB. This would then reflect a signal strength of 15 dB for this remote association. As I am certain you know, regarding availability in remote networks, the specialists express a necessity of an SNR of at any rate 20 dB to state, surf the web. Notwithstanding, the following is SNR prerequisites versus SNR esteems:
5 dB to 10 dB: is underneath the base level to set up an association, because the noise level is almost indistinguishable from the ideal signal (helpful data).
10 dB to 15 dB: is the acknowledged least to build up an untrustworthy association.
15 dB to 25 dB: is normally considered the insignificantly acceptable level to build up a helpless network.
25 dB to 40 dB: is considered to be acceptable.
41 dB or higher: is viewed as superb.

In spite of the fact that SNR is regularly being used to measure the clearness or strength of electrical signals, it can likewise apply to any type of signal (transmission). For instance, it is being used to portray isotope levels in ice centers, biochemical signal-ing between cells, or sound clearness for vehicle amplifiers and source units (DVD, CD, or Digital). In any case, with sound segments, the SNR is consistently a positive worth. For instance, an SNR of 95 dB, implies that the degree of the sound signal is 95 dB higher than the degree of the noise. This, thusly, implies that an SNR of 95 dB is superior to one that is 80 dB.

1.3.2. Calculation of Signal to Noise Ratio

SNR computations can be either basic or complex, and it relies upon the devices being referred to and your access information. Along these lines, on the off chance that your SNR estimations are as of now in decibel structure, at that point you can deduct the noise amount from the ideal signal: SNR = S - N. This is on the grounds that when you deduct logarithms, it is what might be compared to partitioning typical numbers. Additionally, the distinction in the numbers rises to the SNR. For instance, you measure a radio signal with a strength of - 10 dB and a noise signal of - 50 dB. - 10 - (- 50) = 40 dB.

As I expressed before, ascertaining SNR can be included, also. Along these lines, for complex figuring's, you partition the estimation of the ideal signal by the measure of the noise and afterward take the regular logarithm of the outcome, i.e., log (S ÷ N). After this, in the event that the signal strength estimations are in watts (power), you will then increase by 20. Notwithstanding, in the event that they are units of voltage, at that point, you will increase by 10. Furthermore, for power, SNR = 20 log (S ÷ N) and for voltage, SNR = 10 log (S ÷ N). Also, the resulting calculation is the SNR in decibels. For example, your measured noise value (N) is 2 microvolts, and your signal (S) is 300 millivolts. The SNR is 10 log (.3 ÷ .000002) or approximately 62 dB.

1.3.3. Signal to Noise Ratio Formula and Channel Capacity

Signal to noise ratio influences every remote network, and this incorporates Bluetooth, Wi-Fi, 4G, 4G LTE, and 5G, since their operation is subject to radio signals. Additionally,

since they work using radio signals, every one of the referenced specialized strategies has the greatest channel limit. Moreover, as the SNR increments, so does the channel limit. By and large, the channel limit, the transfer speed, and the signal to noise ratio, all influence the most extreme limit of correspondences channels. Additionally, this revelation has a place with Claude Shannon, and he makes this relationship during World War II. In today's fields of gadgets and science, specialists and researchers the same, allude to it as Shannon's Law or the Shannon-Hartley hypothesis.

As per Shannon's Law, the accompanying recipe portrays this connection that shapes the limited subordinate relationship:
C = W log2(1 +)
Within this formula:
C equals the capacity of the channel (bits/s)
S equals the average received signal power
N equals the average noise power
W equals the bandwidth (Hertz).

2. Literature Survey

H. Tang and Z. Ding, 2016, in this paper, in the cell, verbal trade structures with elective device-to-device (D2D) hyperlinks, client hardware (UEs) can work in either D2D mode or cell mode for records transporting. This canvas presents a mixed-mode D2D discussion wherein D2D connections can work in a few modes through asset multiplexing. inside this structure, we experience a glance at the difficulty of boosting weighted D2D total charge underneath cell rate requirements with the guide of streamlining the consolidated mode portion and helpful asset distribution in expressions of communicating power and subchannel adventure. on account of nonconvex cell rate imperatives and parallel limitations of subchannel allotment, this issue is a nonconvex blended number issue this is normally difficult to settle [6].
W. Wang, K. C. Teh, 2017, With this letter, the issue including security for device-to-device (D2D) under-lying cell frameworks are thought of. The versatile report is caught really by arbitrarily dispensed roof droppers. truly by dividing the range between D2D clients and cell phone clients, the obstruction made by D2D customers is utilized as a stockpile identified with sticking to confound commonly the roof droppers. We initially get the relationship opportunity concerning the D2D joins along the edge of the mystery outage opportunity inside the cell connect essentially dependent on stochastic calculation gear [7].

B. Fan, H. Tian, 2018, In this paper, a couple of types of social-cognizant virtual medium advantage gain admission to power (SV-MAC) is made to join virtualization in addition to social-acknowledgment to D2D publicizing and advertising and deals correspondences hidden heterogeneous cell frameworks. SV-MAC is a joined network layer. through SV-MAC, heterogeneous networks can get brought together inside a protocol heap, bestowing a not uncommon être for customers and convenient network operators (MNOs) to have the option to extend their network sources. Utilizing customers' social realities, SV-MAC can understand social-cognizant D2D disclosure, alliance, and even asset assignment for more grounded D2D verbal ex-change execution. in order to approve the advantages with respect to the proposed SV-MAC technique, we notice the portable and D2D help part issues beneath the SV-MAC way [8].
Y. Wu, A. Khisti, C. Xiao, 2018, actual part assurance which shields measurements privacy principally dependent on the particular insights hypothetical techniques has procured large exploration interest nowadays. the significant thing thought driving substantial layer security is normally to use the natural arbitrariness from the transmission channel so one can guarantee the wellbeing within the real layer. The advancement towards 5G remote publicizing correspondences presents new requesting circumstances with respect to actual layer security assessment [9].

X. Lu, D. Niyato, 2018, ordinarily, the fifth generation (5G) remote structures are foreseen to openness charge brought contributions with wherever protection, which makes information insurance uncommonly basic. inside this specific circumstance, actual degree security has arisen because of the reality a promising arrangement with a reason to defend records transmission really through abusing attributes of regularly the remote medium. not-withstanding ordinarily the current innovation improves inner substantial layer security or even remote transmission, mystery power outages (I. e., records penetrates) and supplier blackouts (I. e., association screw-ups) will practically unavoidably show up and get financial misfortunes. This cost-incredible outcome is a demonstrated truth that is commonly disregarded with the guide of the pre-present writing. To offer financial counteraction of mystery blackout and administration blackout, large numbers of us present a digital inclusion plan structure for wi-fi customers in cell networks, in which each shopper can pay a shiny new top rate to an inclusion firm for a future money related reimbursement if a blackout happens to him/her. inside exact [10].

J. Lin, Q. Li, J. Yang, 2018, In this particular paper, they consider commonly the PHY security inconvenience concerning proximal LU and occasion, underneath which some notable PHY protections measures miss the mark to supportive of vide top-notch mystery generally speaking execution in light of the species especially associated LU in addition to Eve channels. To address this, they present various recurrence counterbalances all through the specific exhibit radio wires to decouple the channels, and after that advocate a reformist FDA beamforming procedure. particularly, they incorporate beamforming into FDA, after which reason to augment the exact mystery charge by means of group ly streamlining the recurrence counterbalances in addition to the exhibit send beamformer. To restoration this troublesome issue, the initial offer a few bits of knowledge into the decision of FDA beamforming. and afterward, produce a two-stage strategy that enhances the charge of repeat balances in addition to the communicate beamformer progressively [11].

A. Kuhestani, 2018, in this paper, a joint hand-off decision and force distribution (JRP) conspire are proposed to decorate the substantial layer wellbeing of a helpful network, where more than one reception apparatuses supply speaks with a solitary receiving wire objective in presence of untrusted transfers and aloof busybodies (Eves). The goal is to safeguard the records secretly while simultaneously depending on the untrusted transfers as expected Eves to improve

the security and dependability of the network. To understand this objective, they recall agreeable sticking got done with the guide of the objective while the JRP conspire is done. With the goal of boosting the prompt mystery charge, they infer a spic and span shut structure answer for the best power portion and support a simple hand-off choice measure underneath two circumstances of non-conspiring Eves (NCE) and plotting Eves (CE). For the proposed conspire, a spic and span shut structure articulation is determined for the ergodic mystery rate (ESR) and the mystery blackout likelihood as wellbeing measurements, and another shut structure articulation is provided for the normal image blunder charge (SER) as an unwavering quality measure over Rayleigh blurring channels [12].

Y. Zou, B. Champagne, 2015, they consider an intellectual radio (CR) people group comprising of an optional transmitter (ST), an auxiliary objective (SD), and more than one auxiliary transfers (SRs) inside the presence of a busybody, wherein the ST communicates to the SD with the assistance of SRs, simultaneously as the snoop endeavors to block the auxiliary transmission. they rely upon cautious transfer choice for ensuring the ST-SD transmission contrary to the snoop with the guide of both unmarried-hand-off and multi-hand-off decision. To be explicit, best the "outstanding" SR is chosen inside the unmarried-transfer determination for supporting the optional transmission, while the multi-hand-off choice conjures more than one SRs for at the same time sending the ST's transmission to the SD. they break down each the catch possibility and blackout possibility of the proposed single-hand-off and multi-hand-off choice plans for the optional transmission depending on viable range detecting [13].

F. S. Al-Qahtani, C. Zhong, 2015, on this paper, they present a total examination at the mystery execution of shrewd transfer decision structures employing the interpret and-forward protocol over Rayleigh blurring channels. thinking about a functional putting where an immediate connection between the source hub (Alice) and the place to the getaway hub (Bob) is accessible, they view the mystery generally execution of three distinctive assortment joining plans, explicitly, most extreme ratio consolidating (MRC), dispensed decision consolidating (DSC), and allocated switch-and-live consolidating (DSSC) [14].

B. He and X. Zhou, 2013, real layer security have these days been viewed as an arising technique to enhance and improve the reported wellbeing in future remote networks. The advanced examination and improvement in real layer security are as often as possible essentially dependent on the ideal supposition of best channel skill or the usefulness of variable-charge transmissions. In this paper, they take a gander at the quiet transmission plan in extra viable circumstances by considering channel assessment botches on the beneficiary and examining every steady rate and variable-expense transmissions. Expecting semi-static blurring channels, they plan quiet on-off transmission plans to expand the throughput circumstance to a limitation on mystery blackout likelihood [15].

Y. Zou, X. Wang, W. Shen, 2014, in this paper, they find and look at the tradeoffs between the security and unwavering quality of remote correspondences inside the presence of eavesdropping assaults. usually, the re-obligation of the fundamental connection might be ventured forward by utilizing becoming the source's communicate fuel (or lessening its date charge) to diminish the blackout possibility (OP), which shockingly will expand the danger that a snoop prevails with regards to blocking the source message through the wiretap interface since the OP of the wire-tap interface additionally diminishes while a superior send energy (or lower date charge) is utilized [16].

Y. Feng, S. Yan, Z. Yang, 2018, in this paper, first propose a joint purchaser and hand-off choice (JURS) plan to embellish substantially layer assurance in a multi-individual multi-transfer network, where the top-notch pair of the client and hand-off that amplifies the individual to-objective signal-to-impedance to-noise ratio (SINR) is mutually chosen. they logically view the mystery blackout likelihood (SOP) of this plan, basically dependent on which the ideal energy assignment between the helpful sign and fake noise at the clients is chosen for you to diminish the comparing SOP [17].

2. Problem Statement

Bear in mind the supportive D2D community in view that shown in Fig. 2.a D2D person (A) intends to broadcast private information to another D2D person (B), but the transmission is wiretapped by using an eavesdropper (C). for the reason that transmission in the direct hyperlink is probably to try out an outage, right now there are numerous D2D consumers as relays to help the facts transmission. all the relays exploit the decode-and-forward (DF) protocol and honestly once the channel best concerning A and B might be worse than tolerance, the relays paintings; or else, they may maintain quiet. additionally, the eavesdropper is surely able to wiretap almost all of the information transmitted by actually the relays.

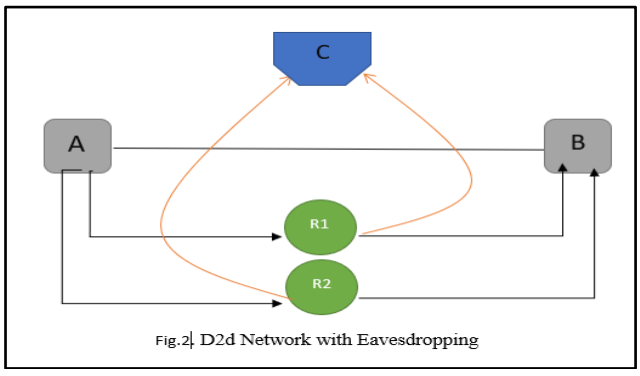

Fig.2| D2d Network with Eavesdropping

3. Proposed System

We propose a novel relay selection and coding method to improve security. We first describe the relay selection scheme and then discuss the coding method. Compared to the existed works that usually select only one relay (e.g., the optimal relay) to help the transmission, our method selects two groups of relays. Users in one of the groups forward private information and users in the other group send artificial noise. By using this method, the signal-to-noise ratio (SNR) at the legitimate receiver is larger than a target value,

but the SNR at the eavesdropper is possibly lower than the target value.

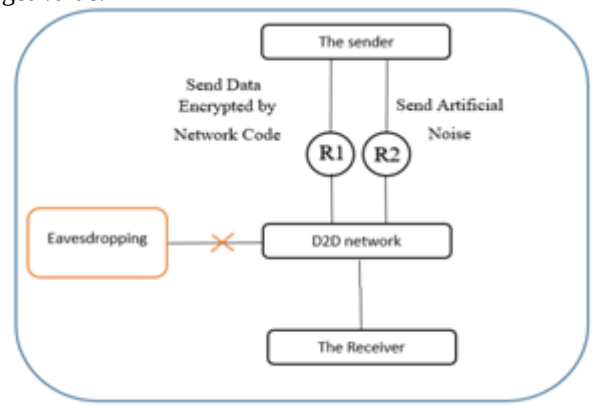

Fig.3| Secure the D2d Network by adding Wyner's and network cod

First the sender will choose tow rely nodes will be in empty rectangle so you can easily identify them then also he should prepare the file for send. Now SNR value > channel rate and eavesdrop also has high SNR rate and it can able to read data so the sender will send on the second rely artificial noise holding a high SNR rate and encrypt the data by network coding so it will be impossible for eavesdropping.

4. Implementation

In network two devices can communicate with each other using signals, one device will encode data into signal and send to destination and if destination is in direct range of source then destination will receive data and decode from signal. If destination not in range of source then destination will receive data with noise and to remove this noise neighbor devices who are in range of source and destination will take data and forward to destination. Sometime some eavesdrop can directly read data from wire and if eavesdrop has good signal then it read entire data from wire flowing from neighbors to destination. In D2D technique we cannot use heavy encryption and we need to provide security without using heavy encryption and key less technique.

To avoid eavesdrop from reading data author is using two relay nodes concept with two techniques called Wyner Coding and Network Coding.

Using Wyner coding we will increase Signal to Noise Ratio (SNR) at destination side and if SNR increases then eavesdrop node cannot able to read data due to more noise. To increase SNR source node will use two relay nodes and from one relay node send normal data to destination (legitimate node) and from other relay node send noise data and destination node read only normal data and ignore noise data but eavesdrop node will think all data is normal data and try to read all data which lead to increase SNR and eavesdrop cannot able to decode all data. Sometime if eavesdrop has high signal or SNR rate then it can able to read data properly by ignoring noise data. No nodes will have prior information about eavesdrop SNR rate, if eavesdrop has high SNR value then Wyner coding will not work and security will be at risk. HIGH SNR rate also called outage security.

To implement above technique, we are designing two applications

1) Data Receiver: This is a data receiver application which accepts data send by source node and then reverse Network Coding can decode data. If same packet receives by attacker then it cannot able to decode data.
2) D2DSimulation: This is a simulation application where we input number of devices and channel rate and then display devices and then find out relay nodes to send data. Here we only need to act like an attacker so randomly I am assigning SNR value to attacker node and if attacker node got high SNR value (greater than input channel rate) compare to given channel rate then it can read data but due to network coding it cannot decode it.

5. Result and Analysis

5.1 Screen Shots of the Simulation

Double click on 'run.bat' file from 'Data Receiver' folder to get below screen

Case 1: Data receiver screen

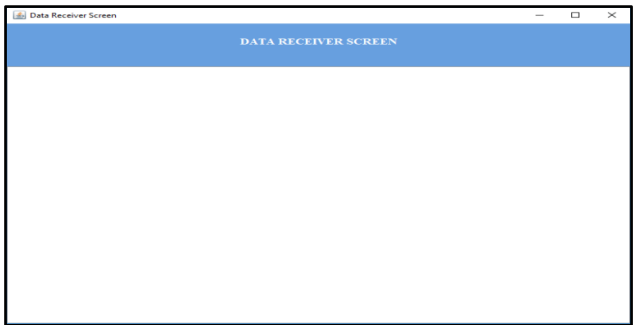

Figure 4: Data Receiver screen

Now let the above screen run and now double click on 'run.bat' file from 'D2DSimualtion' folder to get below screen

Case 3: D2D Parameters Definition screen showing X and Y location

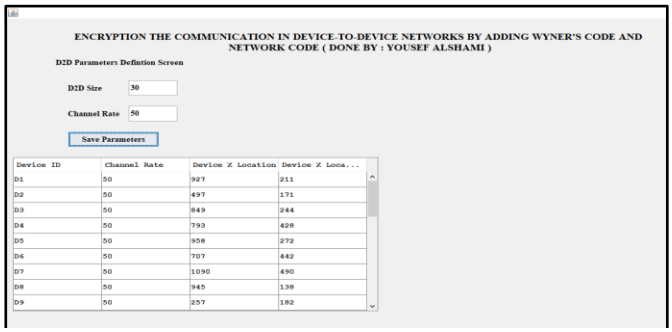

Figure 5: D2D Parameters Definition screen showing X and Y location

In above screen enter device size and channel rate 30 is total no of devices and 50 is the signal which means devices in range of 50 meters can able to read data perfectly. If range >50 then devices will use neighbors. Now click on 'Save Parameters' button to save input values and to get below screen also we can see X and Y location of each device with id and see below simulation screen

Case 4: The mean screen for D2D Relay Group

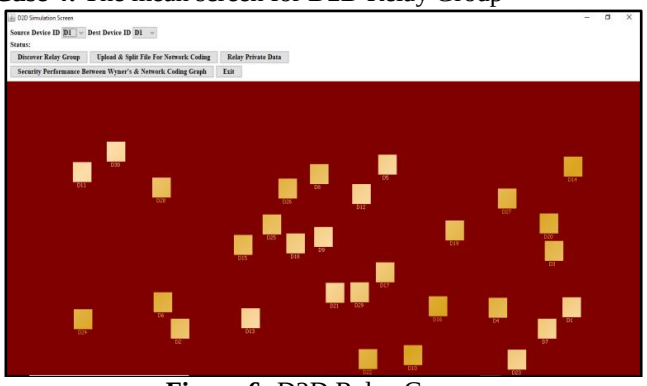

Figure 6: D2D Relay Group

In above screen from drop down box select source and destination device id and then click on 'Discover Relay Group' button to find two best closer relay nodes

Case 5: Discover Relay Group button

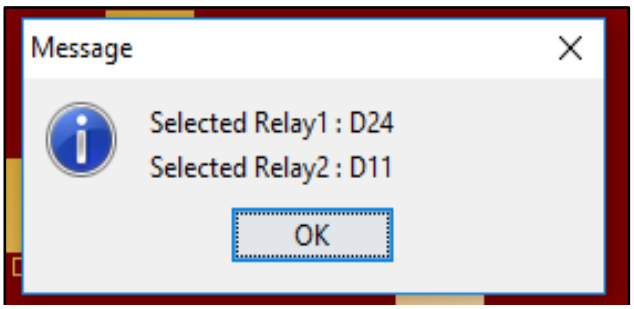

Figure 7: Discover Relay Group

In above screen we can see selected two relay node id and now click ok button to get below screen

Case 6: D2D Relay Group and specific relays for transimation

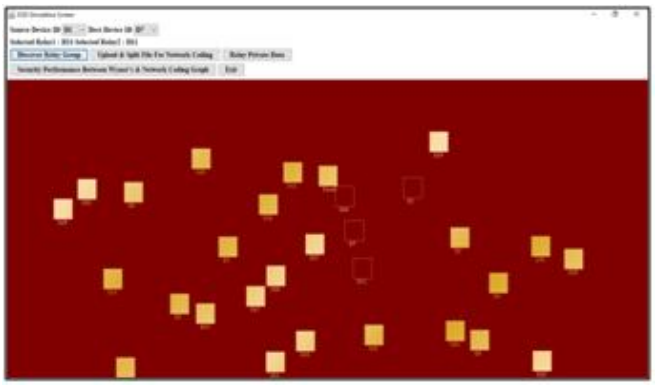

Figure 8: D2D Relay Group

In above screen selected source, destination and relay nodes will be in empty rectangle so u can easily identify them. Now click on 'Upload & Split File for Network Coding' button to upload file and divide to blocks

Case 7: Upload & Split File for Network Coding button

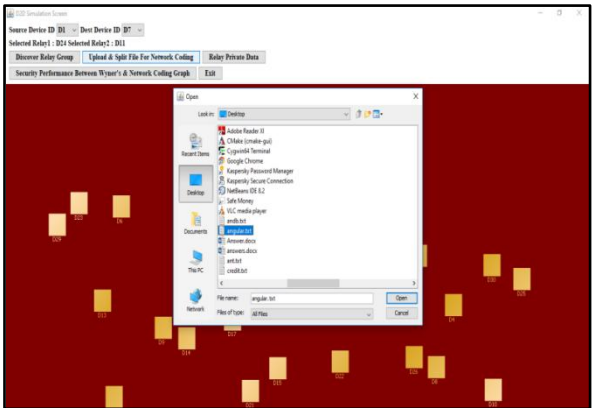

Figure 9: Upload & Split File for Network Coding

In above screen I am uploading one 'angular.txt' file and after upload will get below screen

Case 8: dividing the file into packets before sending

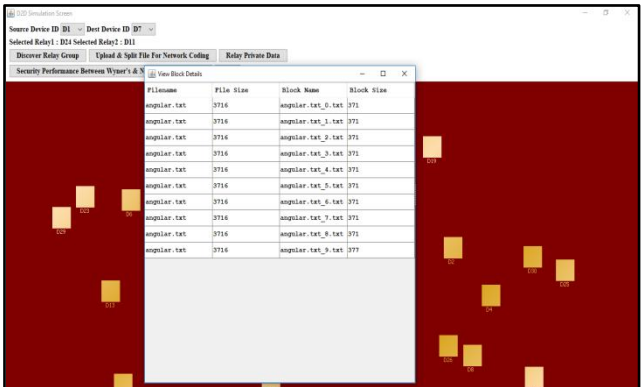

Figure 10: Dividing the file into packets

In above screen we can see single file divided into 10 parts and we can see each part size also. Now click on 'Relay Private Data' button to send this block to destination

Case 9: showing the Relay Private Data

Figure 11: Relay Private Data

In above screen source SNR value > channel rate and eavesdrop also has high SNR rate and it can able to read data. Now click ok button to get next screen

Case 10: reading the data by the eavesdrop node

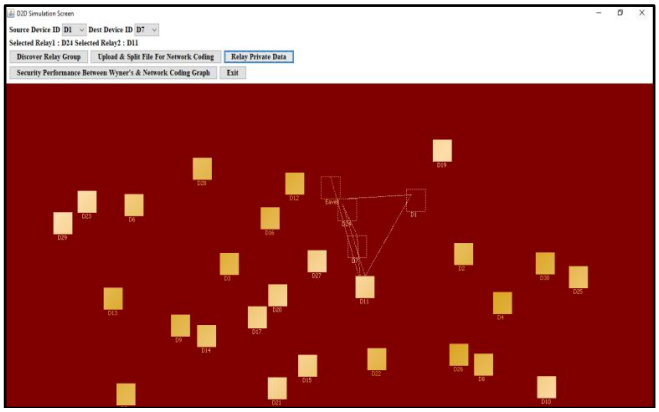

Figure 12: Reading the data by the eavesdrop node

In above screen we can see data sending to destination and at the same time data is reading by eavesdrop node also. The id of attacker node I gave as 'Eaves'. Once data sent to data receiver then two windows will open at 'Data Receiver' side where one window data received by destination and other window data received by eavesdrop node. See below two screens

Case 11: Original file and encryption file

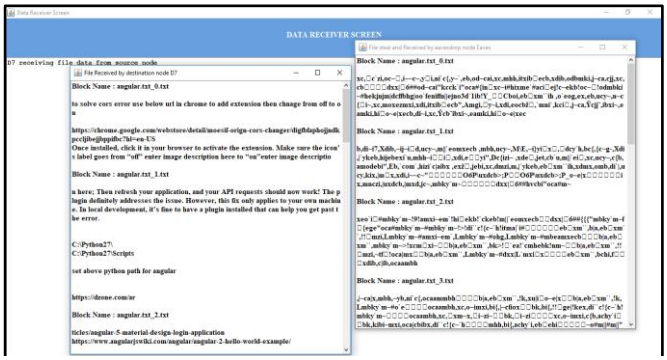

Figure 13: Original file and encryption file

In above screen we can see first window data received by destination and able to decode it properly and second window data received by attacker and unable to decode it.

Case 12: Denay the eavesdrop from accessing data

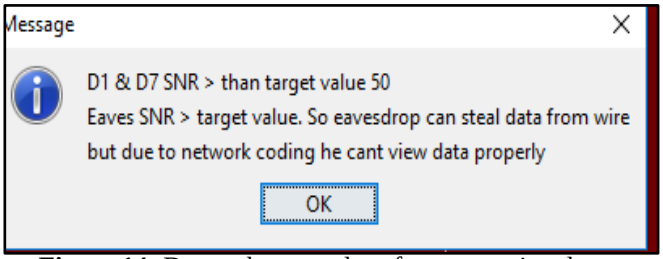

Figure 14: Denay the eavesdrop from accessing data

In above screen if eavesdrop value not > channel then it will display above message. Now click on 'Security Performance between Wyner & network Coding Graph' button to get below graph

6.2. Result Analysis

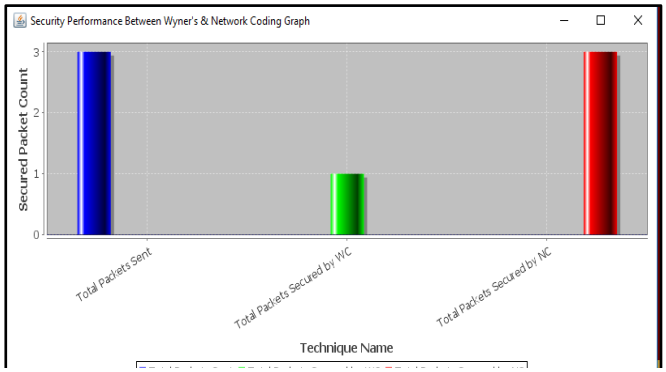

Figure 15: Security Performance between Wyner & network Coding Graph

In above graph x-axis represents technique names Total packets are total packet sent in a network and WC means Wyner Coding which able to secure only 1 packet from total sent packets and NC means network coding which secure all packets. So, using Network Coding outage attack probability will goes down

We further show the relationship between the outage probability and the number of relays. It can be seen that increasing the number of relays can help to ensure the reliability. Thus, if there is enough number of D2D users in the network, the transmitter can increase the transmission rate appropriately.

7. Conclusion

In this paper, we study the safe transmission in helpful D2D networks. A tale hand-off choice plan is proposed, in which two gatherings of transfers are select to send private data and counterfeit noise. The re-lays chose to communicate private data to improve the dependability of the transmission, and the transfers chose to send fake noise to improve the security. In the transfer, determination conspire, worldwide CSI isn't fundamental, and each hand-off just realizes its own CSI, so the plan is anything but difficult to be accomplished. Besides, not the same as the customary physical-layer security strategies that lone utilizing the Wyner's code, we join the Wyner's code and the network cod-ing to additionally improve the security. As shown by the hypothetical and recreation results, the proposed technique can improve security fundamentally particularly when the quantity of messages to be sent is moderately enormous.

References

[1] Y. Feng, S. Yan, Z. Yang, N. Yang, and J. Yuan, "User and relay selection with artificial noise to enhance physical layer security," IEEE Trans. Veh. Technol., vol. 67, no. 11, pp. 10906–10920, Nov. 2018.
[2] X. Liao, Y. Zhang, Z. Wu, Y. Shen, X. Jiang, and H. Inamura, "On securitydelay trade-off in two-hop wireless networks with buffer-aided relay selection," IEEE Trans. Wireless Commun., vol. 17, no. 3, pp. 1893–1906, Mar. 2018.
[3] A. Kuhestani, A. Mohammadi, and M. Mohammadi, "Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive

eavesdroppers," IEEE Trans. Inf. Forensics Security, vol. 13, no. 2, pp. 341–355, Feb. 2018.
[4] H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, "Exploiting fountain codes for secure wireless delivery," IEEE Commun. Lett., vol. 18, no. 5, pp. 777–780, May 2014.
[5] H. He and P. Ren, "Secure ARQ protocol for wireless communications: Performance analysis and packet coding design," IEEE Trans. Veh. Technol., vol. 67, no. 8, pp. 7158–7169, Aug. 2018.
[6] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1923–1936, Dec. 2013.
[7] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," IEEE Trans. Veh. Technol., vol. 63, no. 6, pp. 2653–2661, Jul. 2014.
[8] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," IEEE Trans. Commun., vol. 63, no. 1, pp. 215–228, Jan. 2015.
[9] F. S. Al-Qahtani, C. Zhong, and H. M. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," IEEE Trans. Commun., vol. 63, no. 5, pp. 1756–1770, May 2015.
[10] H. Tang and Z. Ding, "Mixed mode transmission and resource allocation for D2D communication," IEEE Trans. Wireless Commun., vol. 15, no. 1, pp. 162–175, Jan. 2016.
[11] W. Wang, K. C. Teh, and K. H. Li, "Enhanced physical layer security in D2D spectrum sharing networks," IEEE Wireless Commun. Lett., vol. 6, no. 1, pp. 106–109, Feb. 2017.
[12] B. Fan, H. Tian, L. Jiang, and A. V. Vasilakos, "A social-aware virtual MAC protocol for energy-efficient D2D communications underlying heterogeneous cellular networks," IEEE Trans. Veh. Technol., vol. 67, no. 9, pp. 8372–8385, Sep. 2018.
[13] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," IEEE J. Sel. Areas Commun., vol. 36, no. 4, pp. 679–695, Apr. 2018.
[14] X. Lu, D. Niyato, N. Privault, H. Jiang, and P. Wang, "Managing physical layer security in wireless cellular networks: A cyber insurance approach," IEEE J. Sel. Areas Commun., vol. 36, no. 7, pp. 1648–1661, Jul. 2018.
[15] J. Lin, Q. Li, J. Yang, H. Shao, and W.-Q. Wang, "Physical-layer security for proximal legitimate user and eavesdropper: A frequency diverse array beamforming approach," IEEE Trans. Inf. Forensics Security, vol. 13, no. 3, pp. 671–684, Mar. 2018.
[16] A. Kuhestani, A. Mohammadi, and M. Mohammadi, "Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers," IEEE Trans. Inf. Forensics Security, vol. 13, no. 2, pp. 341–355, Feb. 2018.
[17] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, 1975.
[18] A. Agarwal and M. Charikar, "On the advantage of network coding for improving network throughput," IEEE Information Theory Workshop, San Antonio, Texas, 2004.