International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 122 –128

# Improved Secure Data Transmission Approach (ISDTA) in Dynamic Cognitive Radio Network

Anand Ashok Khatri
*Research Scholar*
*Shri. JJT University*
*Churella, Jhunjhunu*
*(Rajasthan)*

Yogesh Kumar Sharma
*HOD, Research coordinator*
*Shri. JJT University*
*Churella, Jhunjhunu*
*(Rajasthan)*

Satish Ramchandra Todmal
*Academic Dean*
*JSPM’s Imperial College of Engineering and Research,*
*Pune, Maharashtra*

***Abstract:***

*Cognitive Radio also termed as CR, an adaptable and reactive radio network technology which is capable of dynamic detection of accessible nodes situated in a wireless spectrum and changing transmission parameters, providing a communication channel which is more direct on the network and increasing network activity. Although current techniques are designed to solve specific problems in some circumstances, these solutions are not sufficiently robust or flexible to ensure safety under complex conditions essential to breaches of security. This research work has given the details about the simulation of ISDTA and its performance. Simulations and experimental setup are carried out for proposed ISDTA, conventional AODV and Insecure AAODV. With comparison under different conditions, the ISDTA provided best performance, under all insecure conventional routing protocols, with higher packet delivery ratio and high network through, the ISDTA aims to be more robust in terms of communication. Thus, it is proposed that ratio will take measures based on these conditions before an attack takes place instead of having some kind of new protection mechanism. Different access scenarios are examined to enable the CS, taking those conditions into account.*

***Keywords:*** *Cognitive Radio Network****,*** *ISDTA****,*** *cognitive security, Performance.*

## I. Introduction:

A wireless mesh network (WMN) is a complex cognitive Radio network that uses various nodes for communication purposes. The specific thing about WMS is that its highly mobile network will constantly interact. Because of the dynamic existence, the nodes continuously change their network architecture [1]. A WMS is more robust and provides consistency than any other. In MWN when one node doesn't work yet another node interacts directly or indirectly with each other so they can exchange their information and preserve their properties. Mesh Network usually uses secure mesh routers to access data, and is also known as an access point for two communication networks. These secure access points (APs) are the key part of WMS, which plays an important role in its communication which cannot be sustained in a stable network. -- AP can link & exchange information through its access point, while mesh network directly communicates through the access point.

CR is used for a WMN to optimize the available resources & use of the spectrum to make them usable for other items. The usage of WMS is to maximize the coverage area, so that it can be used to the limit [2]. Using mesh networks wirelessly, we will be able to lower the difficulty and reduce the cost of wire that is being used in college & company for connectivity purposes. WNS is often used in the business sector where the platform is permanently blocked or inaccessible. It also finds its usage in general areas where different channels are required to move the data. they are extremely efficient and achieving high throughput is their capability. Providing high connectivity between indoor and outdoor networks in this WMN capable of delivering high quality performance without modifying anything between networks and without adding any additional costs is the capability of wireless mesh network. It can also be used in the public sector without any redundancy to provide the accurate data.

Cognitive Radio also termed as CR, an adaptable and reactive radio network technology

ISSN: 2233-7857 IJFGCN

capable of dynamic detection of available nodes in a wireless spectrum and changing transmission parameters which make more wirelessly available communication channels on the network and improve the operation of the radio network.

The Cognitive Radio is an evolving paradigm designed to address the unlicensed spectrum band shortage (2.4GHz and 5GHz). Recent reports by the Federal Communication Commission (FCC) have shown that many licensed spectrum bands, such as the television bands, are underused while the unlicensed one is overcrowded. New emerging systems, such as IEEE 802.22, suggest that such white bands be used for data transmission as long as no licensed users access it [15]. Spectrum is considered a critical and vital tool in the networking environment. The majority of the spectrum needed for wireless communication was allocated. However, the evidence is that there are not enough portions of the spectrum deployed for a considerable time period. This drove the cognitive radio technology invention as a solution to the drawbacks this fixed the allocation of spectrum created. Due to this there is an improvement in the efficiency of spectrum by managing licensed spectrum that are inefficiently used, the radio equipment therefore can detect supply of spectrum in their environment and the unused spectrum (spectrum holes) is invested by licensed primary users (PUs) and reassigned to secondary users (SUs) [16]. Cognitive radio focuses on the principle of allowing unlicensed users to use licensed bands, while ensuring that primary licensed users are given priority. Cognitive radio networks (CRNs) therefore consist of two user groups, licensed users or main users (PUs), and unlicensed users (secondary users) (SUs). Main users get preferential access to the bandwidth. Secondary users have cognitive radio capabilities that allow them to identify and turn to available channels unless a primary user is using them. Secondary users must compensate for the top priority of PUs by instantly detecting their presence and terminating their contacts to prevent any interference with PUs. The aim of cognitive radio networks is to mitigate the spectrum shortage by identifying smarter and more scalable wireless networks that can dynamically maximize spectrum usage [19].

**Objectives:**

1. To study a different routing protocol like spectrum Routing using Joint Dynamic Resource Allocation and Routing Techniques.
2. To study DSR is Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks its gives better result as compare to AODV and DSDV routing Protocol.
3. To implement our improved secure data transmission approach (ISDTA) on top of routing protocols, such as DSR in MANETs to further evaluate its effectiveness.
4. To design a method to identify Malicious Node in network by investigating the feasibility of adjusting our improved Secure data transmission approach (ISDTA) to address Different types of collaborative attacks in MANETs like Sybil, Gray hole or Sybil [19].
5. To use less radio frequency & resources to get the maximum throughput less time.
6. To improve the efficiency of resource allocation to gain the maximum Packet delivery Ratio.

## II. Performance Analysis Parameters:

We considered the following assessment criteria to determine the performance of the proposed mechanism, including:

1. Packet Delivery Ratio (PDR): It indicates how many nodes are received successfully. Suppose PR is the no. of packets received, and let Pexp be the no. of packets received on the network. RFP = RFP (2)

2. Packet Delay Delivery (PDD): This shows how long each (legitimate / malicious) node needs to delay the transmission of incoming packets. PDD = PRT − PGT (4) allows PRT to be the total number of received packets and to be a PGT to the total no. of generated packets.

3. Total number −Trp(5) The overall number or f packets sent to Trp may be specified by NetworkThroughput = N > number of total or f packets Ttp − Trp(5) overall number o f paquets NetworkDistribution: i.e. total number of paquets sent by a source node over the number for a certain period of time received by the destination node.

4. True Positive Rate (TPR) means the degree to which the system is able to recognize the malicious incoming packets as shown under Equation (7): TPR= TP TP+FN (6). This means that the number of packets dropped by a network as malicious after they were detected and reported

ISSN: 2233-7857 IJFGCN

successfully is the True Positive (TP). Therefore, False Negative (FN) is the amount of packets forwarded rather than dropped after they have been misidentified as positive.

5. True Negative Rate (TNR): TNR is a measure of the mechanism's number of valid packages as shown in Equation ( 8), TNR = TN TN + FP (8)

Where a True Negative (TN) is a neutral network identification number of packet forwarded. A False Positive (FP) usually involves a reduction in the number of packets rather than malicious packets subsequently.

## III. RESULT:

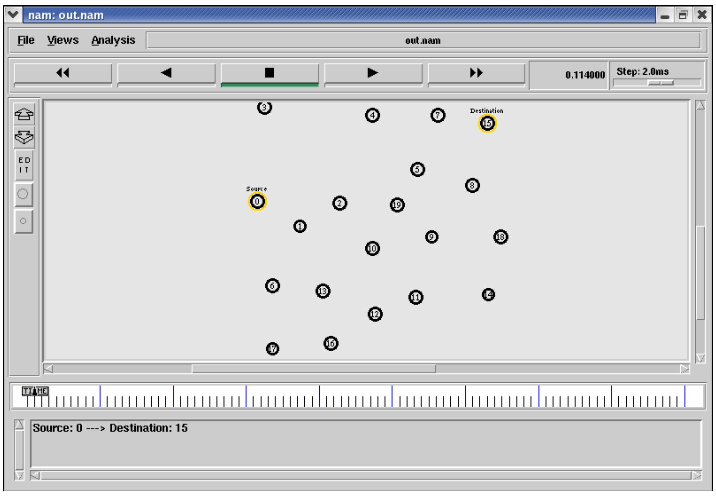
At the network and cognitive layer ensuring a secure routing and communication process is very difficult, this research proposes a trustworthy communication system that not just offers a high confidence among nodes but also provides genuinely affordable services to the user [29]. The 500 m/500 m CRN milieu has separate node numbers as shown in Table 01. Moreover, the suggested hypothesis was validated against malevolent scenarios in which the intruders compromise several legitimate nodes. The CUs were in fact mobile, where they could escape or reconnect at any time from their network. The CU 's mobility rate was set at 0–10 m / s, with 30 m of contact range. The MAC layer protocol that underlies this was also 802.11, while the routers' contact range was set at 120 m. During the communication and handoff process, the CUs or malevolent nodes using the distribution of probability were made to embed into the environment to measure protection.

**Table 01: Parameter use in CRN for simulation**

| Parameters | Values |
|---|---|
| Simulation Time | 80 s |
| Grid Facet | 500 m × 500 m |
| CRN Nodes | 50 |
| Transmission Range | 140 m (approximately) |
| Data Size | 512 bytes |
| MAC Protocol | IEEE 802.11 |

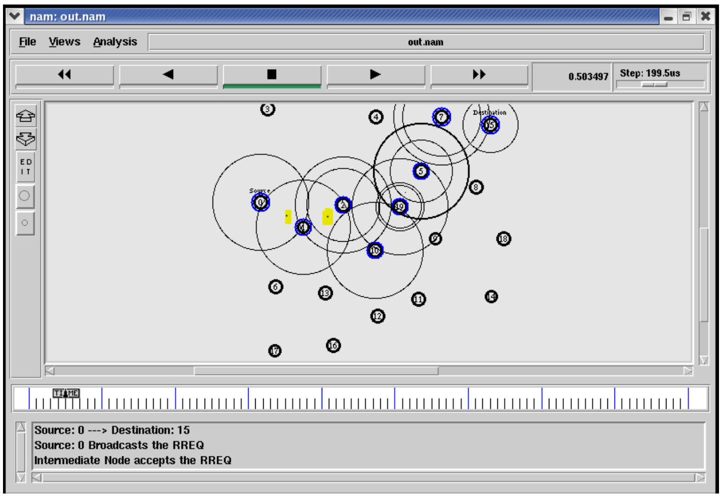
### Simulation:

Performance Analysis of proposed system model namely Energy efficient Clustering Protocol (EECP) in Dynamic Cognitive Radio Network is evaluated and compared with Improve AODV, DSR and DSDV routing protocols based on Packet Delivery Ratio, Processing Delay and throughput to verify, how efficient the implemented secure routing protocol in presence of Sybil attack [19].



Source: 0 ---> Destination: 15

**Figure: Source : 0 & Destination :15**



```
Source: 0 ---> Destination: 15
Source: 0 Broadcasts the RREQ
Intermediate Node accepts the RREQ
```

**Figure: Source Broadcast the Route Request**

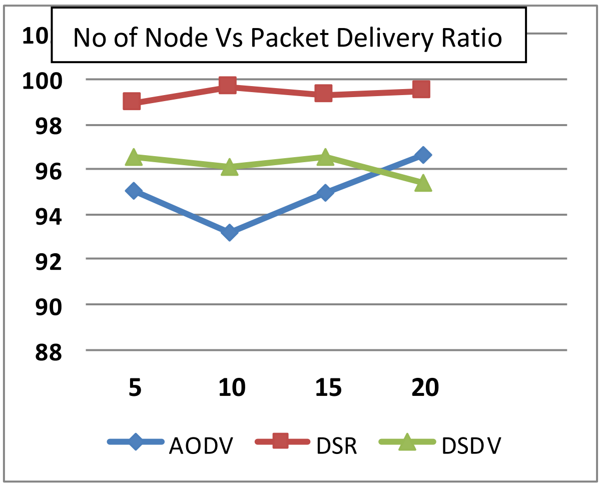
### 3.1 Comparison with ISDTA AODV, DSR & DSDV Routing Protocol:

Performance Analysis of ISDTA AODV, DSR & DSDV Routing Protocol are evaluated and compared based on parameters Packet Delivery Ratio, Processing Delay and throughput to verify, how efficient the DSR routing protocol.

**Packet Delivery Ratio**

| Protocol | Nodes | | | |
|---|---|---|---|---|
| | 5 | 10 | 15 | 20 |
| AODV (ISDTA) | 95.05 | 93.18 | 94.94 | 96.60 |
| DSR (ISDTA) | 98.95 | 99.66 | 99.26 | 99.49 |
| DSDV (ISDTA) | 96.59 | 96.08 | 96.52 | 95.38 |

**Table 2: PDR of ISDTA AODV, DSR, DSDV.**

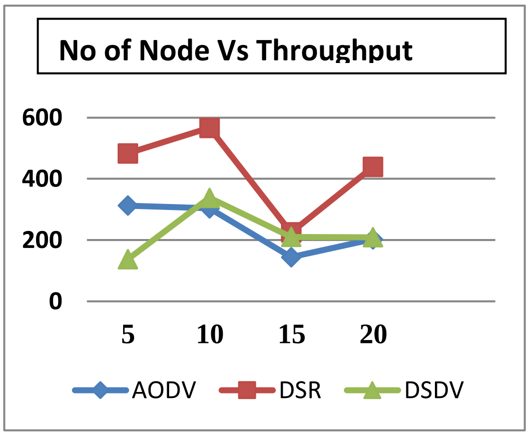


**Graph 1: Comparison of Packet Delivery ratio of ISDTA AODV, DSR, DSDV.**

**Throughput:**

| Protocol | 5 | 10 | 15 | 20 |
|---|---|---|---|---|
| AODV (ISDTA) | 312.56 | 303.79 | 144.12 | 202.3 |
| DSR (ISDTA) | 483.02 | 566.68 | 224.73 | 438.64 |
| DSDV (ISDTA) | 137.01 | 337.99 | 210.50 | 209.02 |

**Table 3: Throughput Of ISDTA AODV,DSR,DSDV.**

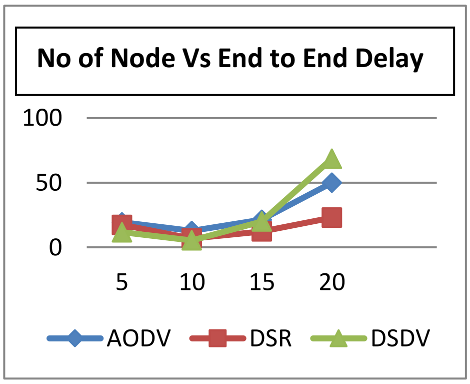


**Graph 2: Throughput Of ISDTA AODV,DSR,DSDV.**

**End to End Delay:**

| Protocol | 5 | 10 | 15 | 20 |
|---|---|---|---|---|
| AODV (ISDTA) | 19.4095 | 12.7261 | 21.344 | 49.9424 |
| DSR (ISDTA) | 17.4164 | 6.87612 | 12.3665 | 23.0443 |
| DSDV (ISDTA) | 11.7883 | 5.47391 | 19.99 | 68.446 |

**Table 4: Comparing E2E Delay of ISDTA AODV, DSR, DSDV.**



**Graph 3: Comparison of E2E Delay of ISDTA AODV, DSR, DSDV.**

## IV. Conclusion:

This research work has given the details about the simulation of ISDTA and its performance. Simulations and experimental setup are carried out for proposed ISDTA, conventional AODV and

Insecure AAODV. The obtained results are compared with DSR and DSDV protocols for its performance evaluation under various parameters. With comparison under different conditions, the ISDTA provided best performance, under all insecure conventional routing protocols, with higher packet delivery ratio and high network through, the ISDTA aims to be more robust in terms of communication. Moreover, the End to End performance with ISDTA is also much low, which comes in an added advantage. This not only increases the node availability but also increases the network performance and minimizes the traffic. Furthermore, the routing throughput of the network in ISDTA is increased. Therefore, the ISDTA protocol proves to be better in many ways, which is set to enhance the wireless Data Transmission Approach in Dynamic Cognitive Radio Network**.**

A detailed NS-2-based comparative simulation study on the performance characteristics of AODV, DSDV and DSR was conducted in this work. Firstly, this work attempted to compare these protocols in an environment of hybrid networking. Following this, the routing protocols On-Demand (DSR and AODV) and Table-Driven (DSDV) were compared by altering the number of nodes and calculating metrics such as end-to - end delay, dropping packets, etc. and presenting the simulation study. It is pointed out from our results that the DSDV is superior to the presentation of the two On-Demand protocols, namely DSR and AODV. It's also found that in less stressful situations DSR outperforms AODV. AODV surpasses DSR in more difficult situation Because of caching and the lack of expiring mechanisms, the weak delay and packet ratio of DSR occurs but with complete production.

The overhead routing of DSR and AODV is consistently low as compared with DSDV. This is because the routing table exchanges will increase in DSDV, with more nodes.

As far as packet delay and dropped packets ratio is concerned, DSR &AODV performs better than DSDV. Hence, for real time traffic DSR is preferred over AODV and DSDV. So, this work proposed to use ISDTA routing protocol for maximum throughput in cognitive radio network.

## Reference:

1. Lee, W. Resource Allocation for Multi-Channel Underlay Cognitive Radio Network based on Deep Neural Network. IEEE Commun. Lett. 2018, 22, 1942–1945.
2. Zheng, M.; Wang, C.; Du, M.; Chen, L.; Liang, W.; Yu, H. A Short Preamble Cognitive MAC Protocol in Cognitive Radio Sensor Networks. IEEE Sens. J. 2019, 19, 6530–6538.
3. Li, S.; Xiao, S.; Zhang, M.; Zhang, X. Power Saving and Improving the Throughput of Spectrum Sharing in Wideband Cognitive Radio Networks. J. Commun. Netw. 2015, 17, 394–405.
4. Ding, X.; Zou, Y.; Zhang, G.; Chen, X.; Wang, X.; Hanzo, L. The Security-Reliability Tradeoff of Multiuser Scheduling Aided Energy Harvesting Cognitive Radio Networks. IEEE Trans. Commun. 2019.
5. Mishra, M.K.; Trivedi, A.; Pattanaik, K. Outage and Energy Efficiency Analysis for Cognitive based Heterogeneous Cellular Networks. Wirel. Netw. 2018, 24, 847–865.
6. Kumar, K.; Prakash, A.; Tripathi, R. A Spectrum Handoff Scheme for Optimal Network selection in Cognitive Radio Vehicular Networks: A Game Theoretic Auction Theory Approach. Phys. Commun. 2017, 24, 19–33.
7. Piran, M.J.; Tran, N.H.; Suh, D.Y.; Song, J.B.; Hong, C.S.; Han, Z. QoE-Driven Channel Allocation and Handoff Management for Seamless Multimedia in Cognitive 5G Cellular Networks. IEEE Trans. Veh. Technol. 2016, 66, 6569–6585.
8. Lu, H.; Zhang, L.; Jiang, M.; Wu, Z. High-Security Chaotic Cognitive Radio System with Subcarrier Shifting. IEEE Commun. Lett. 2015, 19, 1726–1729.
9. Chae, C.J.; Cho, H.J. Enhanced Secure Device Authentication Algorithm in P2P-based Smart Farm System. Peer Netw. Appl. 2018, 11, 1230–1239.
10. Fan, K.; Wang, J.; Wang, X.; Li, H.; Yang, Y. Secure, Efficient and Revocable Data Sharing Scheme for Vehicular Fogs. Peer Netw. Appl. 2018, 11, 766–777.
11. Polese, M.; Giordani, M.; Mezzavilla, M.; Rangan, S.; Zorzi, M. Improved Handover through Dual Connectivity in 5G MMWave Mobile Networks. IEEE J. Sel. Areas Commun. 2017, 35, 2069–2084.

12.Wang, L.C.; Wang, C.W.; Chang, C.J. Modeling and Analysis for Spectrum Handoffs in Cognitive Radio Networks. IEEE Trans. Mob. Comput. 2011, 11, 1499–1513.

13.Nejatian, S.; Syed-Yusof, S.K.; Latiff, N.M.A.; Asadpour, V.; Hosseini, H. Proactive Integrated Handoff Management in Cognitive Radio Mobile Ad-Hoc Networks. EURASIP J. Wirel. Commun. Netw. 2013, 2013, 224.

14.Akilarasu, G.; Shalinie, S.M. Wormhole-Free Routing and DoS Attack Defense in Wireless Mesh Networks. Wirel. Netw. 2017, 23, 1709–1718.

15.YenumulaBG.Reddy," Security Issues and Threats in Cognitive Radio Networks", IARIA 2013.

16.16. Alireza Attar, Helen Tang, Athanasios V., Vasilakos, F. Richard Yu, Victor C.M .Leung," A Survey of Security Challenges in Cognitive Radio Networks: Solution anmd Future Research Directions", Proceedings of IEE,2012,Vol. 100, No 12.

17.TrongNghia Le, Wen-Long Chin, Wei-Che Kao, "Cross –layer design for primary user Emulation Attacks Detection in Mobile Cognitive Radio networks", IEEE communications letter,2015 Vol.19,NO.5.

18. Zesheng Chen, TodorCookley, Chao Chen and Carlos PomalazaRaez,"Modeling Primary User Emulation Attack and defenses in Cognitive Radio Networks,2009,PCCC.2009.5403815.

19.Atul B Kathole, Dr.Dinesh N.Chaudhari, "Pros & Cons of Machine learning and Security Methods ", 2019.http://gujaratresearchsociety.in/index.php/ JGRS, ISSN: 0374-8588 ,Volume 21 Issue 4

20.Atul B Kathole, Dr.Prasad S Halgaonkar, Ashvini Nikhade, " Machine Learning & its Classification Techniques ",International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-9S3, July 2019.

21. Yao Liu,PengNing,Huaiytu Dai," Authenticating Primary Users in Cognitive Radio Networks via integrated Cryptographic and wireless link Signature", 2010, IEEE Symposium on security and PrivacyAltisen, K.; Devismes, S.; Jamet, R.; Lafourcade, P. SR3: Secure Resilient Reputation-Based Routing. Wirel. Netw. 2017, 23, 2111–2133.

22.Ferng, H.W.; Khoa, N.M. On Security of Wireless Sensor Networks: A Data Authentication Protocol using Digital Signature. Wirel. Netw. 2017, 23, 1113–1131.

23.Borkar, G.M.; Mahajan, A. A Secure and Trust based On-Demand Multipath Routing Scheme for Self-Organized Mobile Ad-Hoc Networks. Wirel. Netw. 2017, 23, 2455–2472.

24.Sharifi, M.; Sharifi, A.A.; Niya, M.J.M. Cooperative Spectrum Sensing in the Presence of Primary User Emulation Attack in Cognitive Radio Network: Multi-Level Hypotheses Test Approach. Wirel. Netw. 2018, 24, 61–68.

25.Zhu, C.; Rodrigues, J.J.; Leung, V.C.; Shu, L.; Yang, L.T. Trust-Based Communication for the Industrial Internet-of-Things. IEEE Commun. Mag. 2018, 56, 16–22.

26.Gilbert, E.P.K.; Kaliaperumal, B.; Rajsingh, E.B.; Lydia, M. Trust based Data Prediction, Aggregation and Reconstruction using Compressed Sensing for Clustered Wireless Sensor Networks. Comput. Electr. Eng. 2018, 72, 894–909.

27.Xu, D.; Zhang, S.; Chen, J.; Ma, M. A Provably Secure Anonymous Mutual Authentication Scheme with Key Agreement for SIP using ECC. Peer Netw. Appl. 2018, 11, 837–847.

28.Wang, C.W.; Wang, L.C. Analysis of Reactive Spectrum Handoff in Cognitive Radio Networks. IEEE J. Sel. Areas Commun. 2012, 30, 2016–2028.

29.Wu, Y.; Yang, Q.; Liu, X.; Kwak, K.S. Delay-Constrained Optimal Transmission with Proactive Spectrum Handoff in Cognitive Radio Networks. IEEE Trans. Commun. 2016, 64, 2767–2779.

30. Tayel, A.F.; Rabia, S.I.; Abouelseoud, Y. An Optimized Hybrid Approach for Spectrum Handoff in Cognitive Radio Networks with Non-Identical Channels. IEEE Trans. Commun. 2016, 64, 4487–4496.

31.Liu, X.; Zheng, K.; Liu, X.Y.; Wang, X.; Dai, G. Towards Secure and Energy-Efficient CRNs via Embracing Interference: A Stochastic Geometry Approach. IEEE Access 2018, 6, 36757–36770.

32. Maji, P.; Roy, S.D.; Kundu, S. Physical Layer Security in Cognitive Radio Network with Energy Harvesting Relay and Jamming in the Presence of Direct Link. IET Commun. 2018, 12, 1389–1395.