Data Integrity and Security [DIS] Based Protocol for Cognitive Radio Ad Hoc Networks

Azeem Mohammed Abdul[1], Syed Umar*[2]
[1,2]Department of Electronics and Communication Engineering, KL University, Vaddeswaram, India
[1]Department of Computer Science Engineering, Gandhiji Institute of Science and Technology (GIST), Jaggayyapet, India
*Corresponding author, e-mail: umar332@gmail.com

Abstract

In the CRN (cognitive Radio Networks) the main issues to be addressed are spectrum scarcity and inadequate usage of spectrum. The CRN can analyse the unused spectrum, so that CRN users can easily occupy the unused spectrum without blocking the existing Primary Users. In a CRN, routing is a complex issue because of channel diversity. The existing system mainly focuses on the performance analysis of Ad hoc On-Demand Distance Vector (AODV) and the Weight Cumulative Expected transmission time (WCETT). The performance of these protocols are measured and compared in various ways such as the throughput of single radio station multi-channels, equal number of radio stations and channels, multi-radio stations multi-channels. The limitation with these protocols is, whenever a route fails, there is issue to get connected with the other nodes, the other being data integrity, which maintains the no loss of data [LOD]. In our proposed DIS – CRAHN system we overcome these limitations by adding data security and integrity. Security is provided using the RSA algorithm while Integrity is ensured using the SHA algorithm. With the data security we can maintain the shortest path from source to destination and if any route failure occurs then immediate route establishment can be done and data encryption and decryption also be implemented using the random key generation. Results show an improved performance in delay with reasonable throughput, making the protocol an ideal choice for CRNs.

Keywords: *RSA & SHA algorithm, data security & integrity, data encryption, decryption, AODV, LOD, route maintenance*

1. Introduction

In the present and next generation, Wireless communication and networks play a major role to survive the mankind and their exponential growth leads to the rapid growth of wireless applications for the wireless devices like mobiles, tablets, etc. A survey by the MCMC (Malaysian communications and Multimedia commission) says that there is a tremendous usage of smart devices [1]. Similarly the WWRF (Wireless World Research Forum) outlined that nearly seven trillion smart devices will provide services to seven billion people as a vision from them in next coming years. By this we can clearly say that the usage of spectrum increases with increasing number of devices. With the usage of more spectrums, apparently there will be network data traffic congestion and overloading which make data transmission more delayed [2]. In the maximum cases, wireless networks will use only the fixed spectrum which is allocated to them. FCC (Federal Communications Commission) is the Organization primarily responsible for synchronizing the usage of resources of radio Spectrum. However, the CRN may still fail under the unlicensed users which use dynamic access techniques. These have very good capabilities like usage of full spectrum as shown in Figure 1, and can easily alter the parameters like frequencies, power utilization and data transmission rate to be very reliable and to satisfy the user`s requirements. Therefore, the performance of routing protocols AODV and WCETT has been compared in the presence of unlicensed users. A comparison of AODV and WCETT has been mentioned in [3] related to CRAHNs. The work is done in the presence of a number of different channels, and a radio receiver.

Results show that the total throughput in WCETT has is better compared to CRAHN efficient AODV in case of multichannel multi radio systems. Two new routing protocols [4] CR-AODV and ROPCORN CR-AODV [5] are analyzed and compared to the current multi-radio-end

Received July 15, 2016; Revised October 10, 2016; Accepted November 2, 2016

multi-channel AODV (AODV-MM) ROPCORN for the bandwidth and end to end delay.

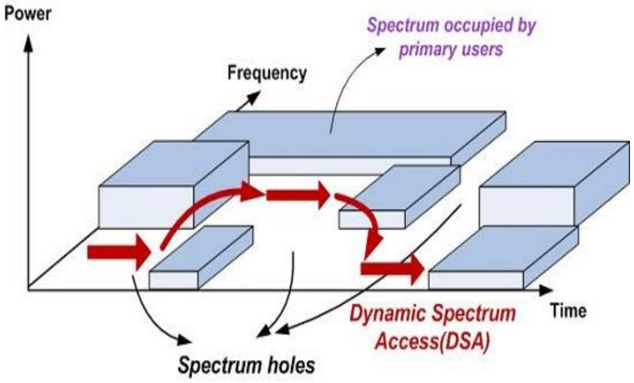
Power
Spectrum occupied by primary users
Frequency
Time
Dynamic Spectrum Access(DSA)
Spectrum holes

Figure 1. CRN Analysis

2. Adhoc Networking in Cognitive Radio

In cognitive Radio networks, Adhoc networking will be used to overcome the channel diversity. These networks are called as Cognitive Radio Adhoc Networks [CRAHN]. These are characterised by multi-hop architecture in distributed manner, dynamic topologies and can operate on wide range of frequency spectrum both in time and space, when compared with classical adhoc networks. To develop more robust networks and architectures, researchers are focusing on algorithms for clustering mechanism which can be implemented at the DLL [Data link Layer] of CRN. By this there will high efficiency in network management and allocation of resources. The Main focus of this work is to deal with the following issues in a CRAHN:

1. Routing in Cognitive Radio
2. Topology Control in Cognitive Radio
3. Efficient Data transmission and reception in Cognitive Radio
4. Managing QoS in CRN

2.1. Routing Structure in CRAHN

In the CRAHN the infrastructure is based on the central network entity which will be the centre point from access node or the base station for data transmission and reception. In this network there will be direct mode of communication from one CR node to other CR node on unlicensed networks or licensed networks. When we compare the CR network users with the primary network users, CR network users have a facility to use both the licensed and unlicensed spectrum bands for communication using multi-hop mode.

2.2. Routing Protocol in CRNs

In the dynamic topology of adhoc networks, the most challenging limitation is routing from main node to target node. In MANETS, routing protocols are classified as Proactive (table driven), Reactive (On demand) and hybrid (combination of both) routing protocols [7]. In the AODV protocol, there will be high rate of average throughput over the channel for broadcasting messages. Apart from AODV the other protocol based on WCETT gives maximum throughput which will meet the CRN requirements. A comparison of both these protocols is given in [8]. In this paper, we propose a protocol DIS-CRAHN, a modification of the CR-AODV protocol and compare the same with CR-AODV and the CR-WCETT for performance.

2.3. CR – AODV

In the general AODV protocol, the route will be laid based on the demand from main node to target node with the help of some messages like Route Request, Reply, Error & HELLO [ACK] which is shown in Figure 2 [8]. The process will be initiated whenever the main/ source node sends route request RREQ messages/packet to the surrounding nodes which will unicast reply messages/packet as RREP to the sending node, provided they have a route to the destination, through a channel which is free from Primary user activity. If the sequence number of the RREQ for the destination is greater than that of an intermediate node, the intermediate node rebroadcasts the RREQ along the same channel. When additional route request arrives along the same channel, it is checked and if the same RREQ arrives, it is assigned to the best reverse route among the routes stored in the routing table. This way, once the total path is laid, among all the paths it will find the shortest path and start transfer of data from source to destination nodes [9].

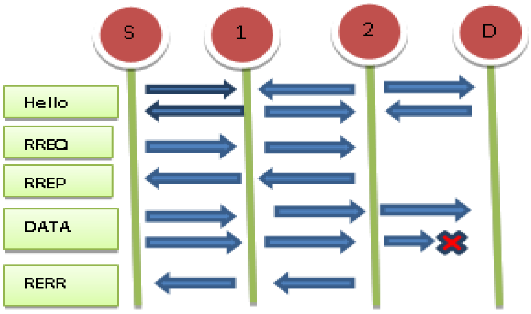

Figure 2. Routing analogy in CR-AODV

2.4. CR - WCETT

The Weighted Cumulative Expected Transmission Time protocol is similar in operation to the AODV protocol [8]. The functionality and working are similar but it differs in the selection of the best and shortest route from source to destination. When the Route request RREQ packets are sent to the receiver, route reply packet will be received as ACK and immediately communication starts [9]. In this protocol, the WCETT values for new RREQ packets are stored in a routing table. When new RREQ packets are received, if their WCETT value is smaller than that of the RREQ packet with the same sequence number, it is forwarded. The path with the least transmission cost is selected by the source for data transmission

2.5. Limitation of CR-AODV & WCETT

During the path routing and after the establishment of route from main node to target node, some issues related to Route security, viz., Data Security and data Integrity are raised. In this paper, these two issues in CR-AODV are addressed. The reason to implement the data security is that the CR networks, also called as Emergency Networks, need to establish connection immediately during the military emergency or during the natural disasters. As the usage of Cognitive Radio networks is more in military communication, at the time when the network is formed, if security is not maintained, then hacker nodes will enter and capture the data which is transmitted and received. The potential solution we suggest is to use the SHA and RSA algorithm to encrypt and decrypt the data when transmitting and receiving the data at nodes respectively. During the encryption of data while transferring, a key will be produced and whenever the key matches, only then data will be decrypted at the receiver node. In a CRN, there should be very less delay when transferring the data from sender to the receiver node. This objective is met as discussed subsequently in the results section.

3. Implementation of Data Integrity & Security in our Proposed System [DIS- CHARN]

In a CRN some issues like channel diversity exist, that can be overcome by the CR-AODV routing protocol which will be used to find the best and shortest route from source to destination. Although CR-AODV solves this problem, during data transmission, necessary steps are to be taken to prevent an intruder in the routing path. In the presence of intrusion, the data which is transmitted by a node will be hacked by some other networks. To overcome this, we introduce some cryptographic techniques by which the data can be encrypted and decrypted during transmission and reception respectively. In this paper, to overcome such issues we use two algorithms for data security.

The two algorithms are:

1. RSA Algorithm
2. SHA Algorithm

3.1. RSA Algorithm for Encryption

The RSA algorithm [11] [12] is the one which is used for the generation of public key and private key during transmission of data. It involves in four steps a) Generation of Key (public or private). b) Distribution of Key c) Data Encryption and d) Data decryption. The public key will be known to all, but the private key which is generated during the data encryption will be sent to the receiver node and a reasonable amount of time will be allotted to decrypt the data. The RSA algorithm is based on finding the parameters e, d, and n with the modular exponential to m as in equation 1. Equation 1 can also be written as equation 2 by interchanging d and e values.

$$(m^e)^d \equiv m(\bmod n) \qquad [1]$$

$$(m^d)^e \equiv m(\bmod n) \qquad [2]$$

The sender A can send encrypted message to B without the need for prior exchange of secret keys. A will transmits her public key (*n,e*) to B on a route which is reliable. For Encryption, let`s consider an integer 'm' that lies between (0,n) such that gcd of {m,n} should be equal to 1. From m and n, it computes the cipher text c shown in equation 3. By this encryption of data is successful. When B sends the data to A, in the Decryption process, *m* is recovered from c using the private key exponential *d* by the eqn 4.

$$c \equiv m^e(\bmod n) \qquad [3]$$

$$c^d \equiv (m^e)^d \equiv m(\bmod n) \qquad [4]$$

3.2. SHA Algorithm

The SHA algorithm uses cryptographic hash functions. The main application of SHA [13] [14] is that it produces cryptographic fingerprints for a message, similar to storing of passwords and is affected minimally by the collision attack. This is because of the fact that a minor change in a moderately lengthy text produces a hash key that vastly differs from the previous key. The hashes generated by the SHA algorithm will be more secure as long as different message inputs do not produce the same hash resulting in a collision. SHA was determined to be more resistant to collisions than the MD5 algorithm.

Both RSA and SHA algorithms are used in our work for encryption and decryption of messages over the selected channels for communication.

4. Implementation of DIS-CRAHN

In the proposed DIS-CRAHN protocol, the parameters added to the RREQ message in the CR-AODV protocol are: request for Random/ Session key from Source to destination and ertificate of sender and Generation of Public Key

To the RREP message from the destination to the source the additional messages added are:

1. Request for the Random/ session key
2. Certificate and public key from destination.
3. Generation of Random key with Random Prime numbers.

The Random key will be received at the source and will be passed to the application layer in the network. The routing and exchange of keys can be done from both sides. By this the routing path is set with high security and there will be no loss/damage of data when transmitted from the source to receiver. The delay corresponding to the packet deliver ratio will be very less compared with the existing the system which is shown in the Figure 2.

The practical implementation of the DIS-CRAHN is described by Level 1 to 4 Data Flow Diagrams (DFDs). In each level we describe the implementation of the proposed protocol.

4.1. Level 1

In the level 1, the performance analysis of the CR-AODV routing protocol for CRAHN is done (Figure 3). The protocol is tested for various parameters such as with single channel, with multiple channels and the simulation results are shown.

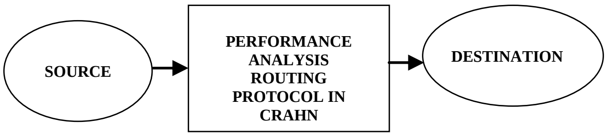

Figure 3. Level 1 Implementation of DIS-CRAHN

4.2. Level 2

In the Level 2, shortest route from source to destination is found. The implementation is shown in Figure 4. After finding the best path, the data will be transmitted from source node to destination node along the path.

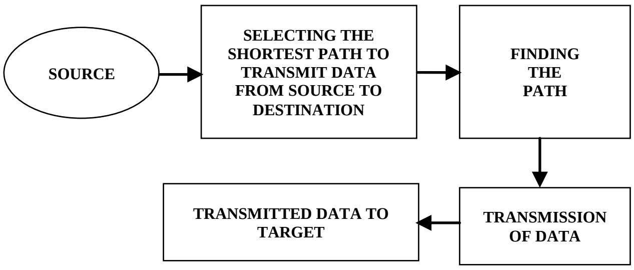
SOURCE
SELECTING THE SHORTEST PATH TO TRANSMIT DATA FROM SOURCE TO DESTINATION
FINDING THE PATH
TRANSMISSION OF DATA
TRANSMITTED DATA TO TARGET

Figure 4. Level 2 Implementation of DIS CRAHN

4.3. Level 3

In the Level 3, the data security implementation begins. The implementation flow is shown in Figure 5. In this level after selection of shortest path from source to destination, the encryption of data will begin using the SHA & RSA algorithm where the public and private key will be generated and will be sent to the destination.

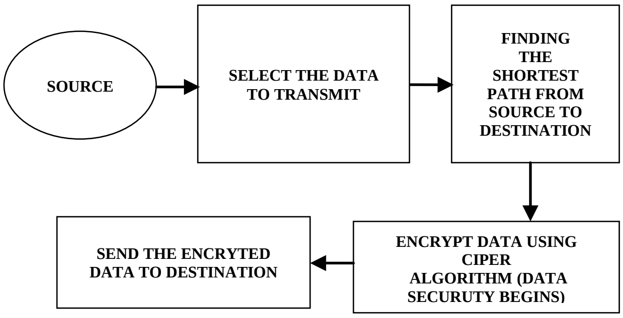
SOURCE
SELECT THE DATA TO TRANSMIT
FINDING THE SHORTEST PATH FROM SOURCE TO DESTINATION
ENCRYPT DATA USING CIPER ALGORITHM (DATA SECURUTY BEGINS)
SEND THE ENCRYTED DATA TO DESTINATION

Figure 5. Level 3 Implementation of DIS-CRAHN

4.4. Level 4

This is the final level where the link availability and expiry analysis is done. If available, then the data is transmitted to destination and will be decrypted and the data packet will be used. The flow of level four is shown in Figure 6.

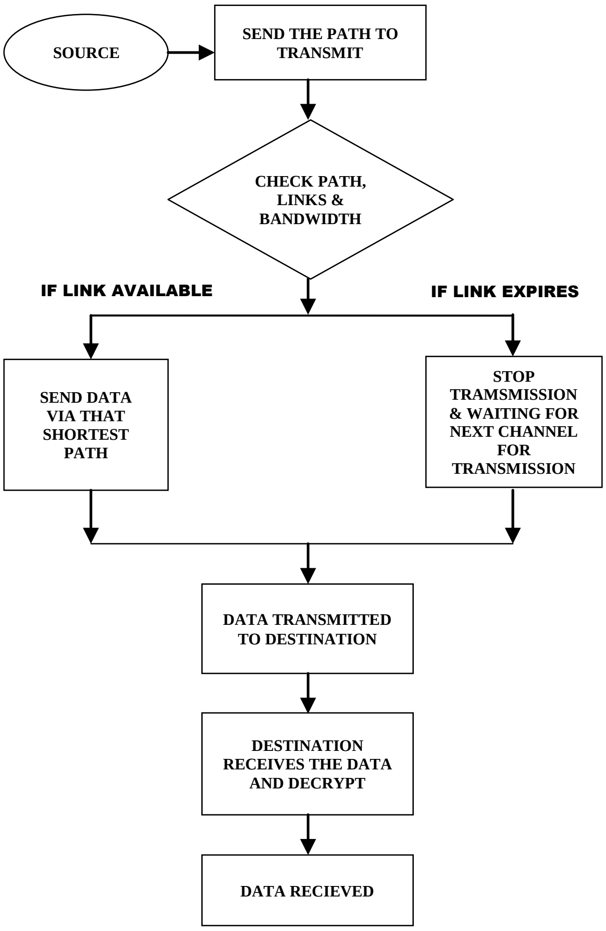
SOURCE
SEND THE PATH TO TRANSMIT
CHECK PATH, LINKS & BANDWIDTH
IF LINK AVAILABLE
IF LINK EXPIRES
SEND DATA VIA THAT SHORTEST PATH
STOP TRAMSMISSION & WAITING FOR NEXT CHANNEL FOR TRANSMISSION
DATA TRANSMITTED TO DESTINATION
DESTINATION RECEIVES THE DATA AND DECRYPT
DATA RECIEVED

Figure 6. Level 4 Implementation of DIS-CRAHN

5. Simulation Analysis and Experimental setup

The simulation has been performed using the NS2 simulator. The simulation parameters considered are- a network topology area of 1000*1000 sq.m, traffic type FTP, packet size 512b, simulation duration of nearly 50 sec. The performance of DIS-CRAHN, CR-AODV and CR-WCETT are examined and compared using multiple random topologies.

5.1. Single Radio Multi-channel

The CRN routing performance with single radio and multi-channel is shown in Figure 7 and the throughput of CR-AODV is compared with that of CR-WCETT. CR-AODV has higher overall throughput than the CR-WCETT. CR-AODV starts dominating in the throughput of CR-WCETT at 100.000, 360.000 point with 100.000, 344.000 CR-AODV has nearly 16% higher effective throughput than the WCETT. From this graph we can say that CR-AODV is much more efficient in the overall throughput than the CR-WCETT. In the DIS-CRAHN is showing 9% [100.000, 369.000] more efficient than the CR-AODV. So when security is maintained in data transfer there is good enough throughput which is shown below in Figure 7 graph.

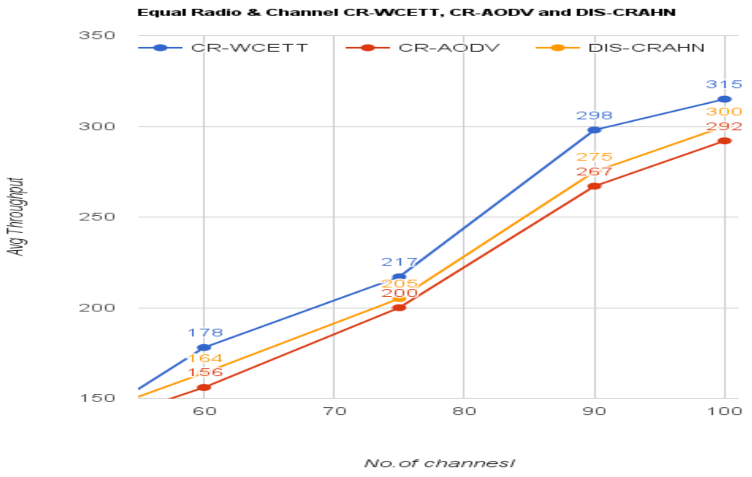

Figure 7. Single Radio station and Multi-Channels Simulation in DIS-CRAHN

5.2. Equal Number of Radios & Channels

The CRN routing performance comparison for equal number of Radios and multiple-channels is shown in Figure 8. From this graph we shows, throughput of CR-WCETT more efficient than the CR-AODV with 23%. When compared with CR-AODV the DIS-CRAHN is 8% efficient but when compared with CR-WCETT it is 15% less throughput. This is shown in the graph in Figure 8.

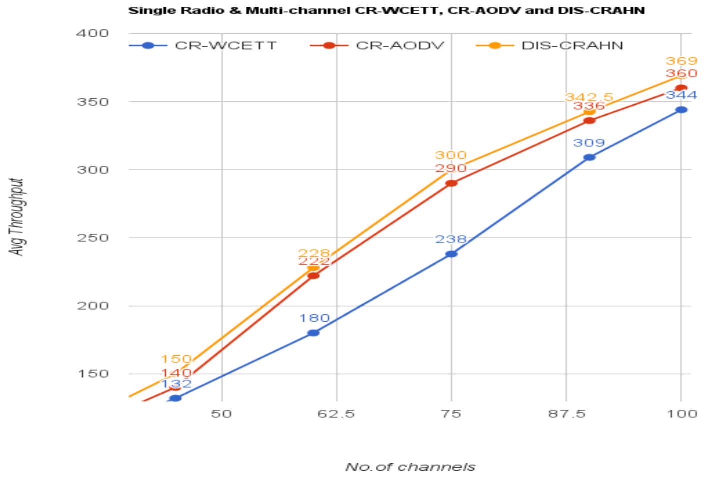

Figure 8. Equal Radio stations and Channels Simulation in DIS –CRAHN

5.3. Multi-Channel & Multi Radios

In next case, for multi-channel and multi radios, increase in the number of channels results in CR-WCETT throughput better than the CR-AODV which is shown in Figure 9. From the graph it can be analysed that at initial point itself, for CR-AODV [5,96] and CR-WCETT [5,103], the peak level in throughput is reached and the difference in percent is nearly 7%, that for CR-WCETT] being higher. Here when compared with CR-AODV [5,96] and DIS-CRAHN [5,99] it is 3% efficient but when compared DIS-CRAHN with CR-WCETT it is 5% less efficient of throughput which is shown in graph below Figure 9.

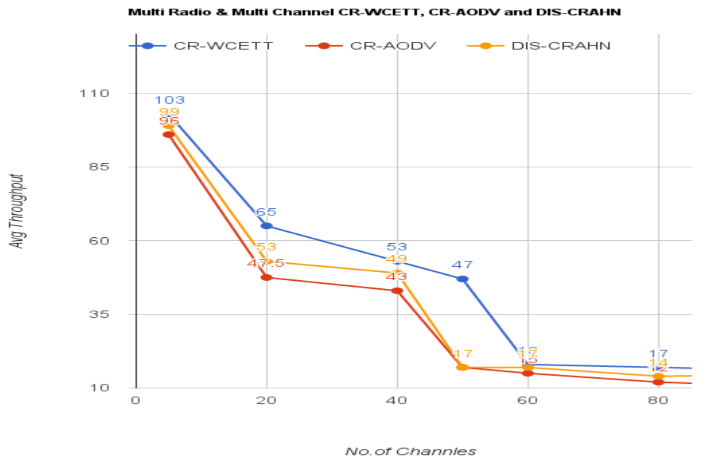

Figure 9. Multi Radio stations and Multi-Channels Simulation in DIS -CRAHN

5.4. Delay Analysis

The Delay analysis is also simulated for the data transmission while maintaining data integrity. Data security is maintained using the RSA and SHA algorithms. In the graph in Figure 10 we compare the transmission characteristics for CR-AODV without the data integrity and security and with the implementation of the same in DIS -CRAHN. DIS-CRAHN is observed to have lesser delay compared to the CR-AODV. For nearly the same packet delivery ratio, the delay is 679 ms for the existing CR-AODV and for DIS-CRAHN, the delay is 550.000 ms, difference being nearly 129.00 ms. The lesser delay can be attributed to the data security and integrity in the proposed DIS-CRAHN.

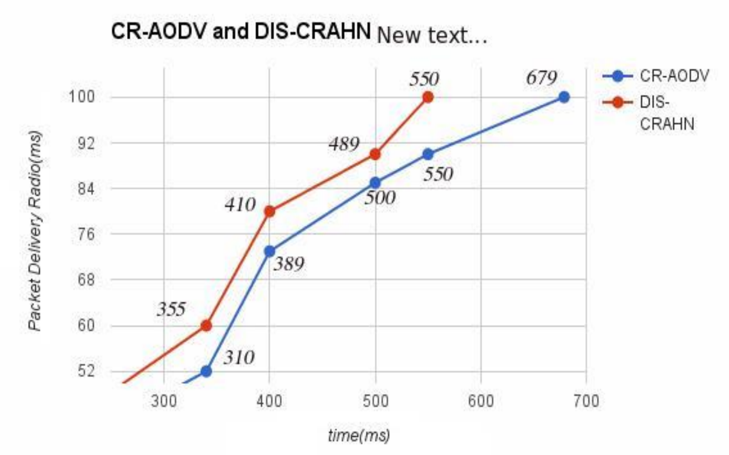

Figure 10. Delay Analysis of existing system and the proposed system [DIS-CRAHN]

6. Conclusion

In this paper, we propose a routing protocol DIS-CRAHN that incorporates data security and integrity in the existing CR-AODV routing protocol. We compare the performance with both CR-AODV and CR-WCETT protocols for throughput and delay with different number of Radios and Channels. The proposed algorithm achieves efficient data transmission with high data security using cryptographic techniques based on the RSA and SHA algorithms for encryption and decryption of the data transmitted from source to destination. By adding data security in CR-AODV route stability is maintained and if any route failure occurs then immediate alternate path will be laid. With proposed data integrity and security mechanism, the packet/data transfer ratio will be more and the delay is less compared with CR-AODV since there will be no data loss or damage. The throughput of the proposed system was observed to be in between that of CR-AODV and CR-WCETT protocols.

References

[1] WCC MIMOS Berhad. *Cognitive Radio Technology: A Survey*. My Convergence. 2011: 36–42.

[2] S Haykin. Cognitive radio: brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications*. 2005; 23(2): 201–220.

[3] R Rai, V Tiwari and S Kansal. Comparison of Routing Protocol AODV and WCETT in Cognitive Radio Network. *International Journal of Engineering.* 2013; 2(10).

[4] A Chehata, W Ajib and H Elbiaze. An On-Demand Routing Protocol for Multi-Hop Multi-Radio Multi-Channel Cognitive Radio Networks. in *Wireless Days (WD),* 2011 IFIP. 2011: 1–5.

[5] A Cagatay Talay and DT Altilar. ROPCORN: Routing Protocol for Cognitive Radio Ad Hoc Networks. in *International Conference on Ultra Modern Telecommunications Workshops*, 2009. ICUMT '09. 2009: 1–6.

[6] R Kaur and MK Rai. A Novel Review on Routing Protocols in MANETs. *Undergraduate Academic Research Journal (UARJ)*, ISSN. 2012: 2278–1129.

[7] NYG García and DAL Sarmiento. *Evaluation of Protocol Applied to Network Routing WCETT Cognitive Radio*. in Proceedings of World Academy of Science, Engineering and Technology. 2012.

[8] S Singhroy, PL Zade and N Bodhya. Comparative Analysis of AOMDV, AODV, DSR and DSDV Routing Protocols for Cognitive Radio. *International Journal of Electronics, Communication & Instrumentation Engineering Research and Development (IJECIERD)*. 2013; 3(2): 1–6.

[9] S Patel. An On-demand Routing Technique for Cognitive Radio Ad Hoc Network. *International Journal of Engineering*. 2013; 2(5).

[10] Rivest R, Shamir A, Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems (PDF). *Communications of the ACM*. 1978; 21(2): 120–126. doi: 10.1145/359340.359342

[11] Johnson J, Kaliski B. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. 2013. www.ietf.org. Network Working Group. Retrieved 9 March 2016.

[12] Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger, MD5 considered harmful today: Creating a rogue CA certificate, accessed March 29, 2009.