DOI 10.29042/2018-3383-3393

Helix Vol. 8(3):3383-3393

CSR-AODV: A CRYPTO SECURED ON-DEMAND ROUTING PROTOCOL FOR COGNITIVE RADIO AD HOC NETWORKS

Chandra Sekhar Musinana [1,*], Kalyana Chakravarthy Chilukuri [1], Prasad Reddy PVGD [2]

[1]Department of Computer Science and Engineering, M.V.G.R College of Engineering (Autonomous), Affiliated to JNT University, Kakinada, India, [2] Department of Computer Science & Systems Engineering, College of Engineering, Andhra University, Visakhapatnam, India

***Email:** chandrasekhar.m@mvgrce.edu.in*

Received: 11th October 2017, Accepted 17th March 18, Published: 30th April 2018

Abstract

Cognitive Radio Ad hoc Network (CRAHN) was a versatile, intuitive radio and network technology that can sense the available channels in the wireless spectrum and will adjust the transmission parameters in a way that it can have multiple communications to run in parallel and also will help to improve the behavior of radio spectrum. In the CRAHN there are many issues that needs to addressed major of them being spectrum scarcity due to the fact that the range of this network will be very short for which we cannot allocate much spectrum as there will be a possibility of not using it or reserving it for Primary Users (PU's) who may not be active at all times and if we allocate more spectrum at peak times it could be advantage but at majority times it will be unused. We have done a comparative study on various available protocols and found that AODV is close to address the above issue. In AODV (Ad hoc on Demand Vector Routing) is a category of Reactive protocol where it will not keep track of any route. The route will be just established whenever any intermediate node has some data to send. Once the data gets successfully transmitted then it will no longer record the address. This property is carried out with the help of maintaining sequence numbers between every pair of nodes. The existing system CRAODV-S mainly focused on security based on trust values, where the mechanism of assigning this value was given based on the Secondary Users(SU's) activities. If the trust value was a bit high than the threshold value then it will be chosen for transmitting messages compared to the remaining nodes with less trust value. This trust value will not be assigned to Primary Users as they will be trusted parties for the network. Based on this trust value the nodes can be categorized as healthy nodes and malicious nodes. The routing also depends on the trusted value of the neighbors for forwarding or receiving a message. In our proposed model CSR-AODV for better security and integrity we have implemented cryptographic techniques in terms of security by using RSA-32 bit and integrity using SHA-III for minimizing the loss of data. Security characteristic is provided by selecting the best optimal route from source to destination and when any intermediate route or node fails then to establish another route for this message transmission is carried out using random key generation. The performance of CSR-AODV and CRAODV-S is assessed for three kinds of routing structure in terms of average throughput, end to end delay, packet delivery ratio and routing overhead for satisfying different requirements from users. The routing structures on which the experiment was carried out are a) Single radio multi-channels b) Equal number of radios and channels and c) Multi-radios multi-channels. The simulation result shows that our proposed model gave significant improvement in all performance metrics except for the case of average throughput in single radio multi channel. So this model will be an ideal choice for CRAHN.

Key words: *CRAHN, AODV, Trust Values, CRAODV-S, Security, RSA 32 bit, Integrity, SHA-III.*

Introduction

Cognitive Radio Networks are capable of effective utilization of the spectrum band that has become a scarce resource of late for wireless networks. They use Cognitive Radios for this purpose. The term 'Cognitive Radio' was introduced by 'Joseph Mitola'. So it is also called as 'Mitola Radio' [1]. The cognitive radio has two characteristics - Cognitive Capability which is sensing vacant spectrum by using sophisticated methods such as autonomous learning and reconfigurability which enables using different spectrums for sending and receiving data by using different data access technologies. With the help of these two characteristics, cognitive radio makes use of spectrum holes which are the unused unlicensed band of frequencies [2]. When a primary user comes back, the secondary user should vacate the channel without interfering [3].

The cognitive radio network has three major functionalities: sensing, analysis and decision [4].Cognitive Radio senses information of spectrum holes using two methods - Non Cooperative Spectrum Sensing in which cognitive radio acts on its own itself and Cooperative Spectrum Sensing in which different cognitive radios senses the spectrum holes and send the information to a central station where an optimistic spectrum band is allocated based on the availability of frequency, time slots, etc., of secondary users. In addition to these two spectrum sensing methodologies, cognitive radios sense vacant spectrum bands based on bandwidth,

transmission type, accuracy and timing window. Cognitive Radio accesses the unused spectrum without interfering with the primary users who has the highest priority to access and can change the parameters based on the conditions of wireless environment to decide which spectrum hole to occupy in order to satisfy its Quality Of Service (QOS).

CRAHN Architecture & Routing Structures

Cognitive Radio Network Architecture can be both Infrastructure based as well as Infrastructure less the latter is commonly referred to as a Cognitive Radio Ad-Hoc Network [5]. The communication among nodes in Infrastructure Based CRN is monitored by an access point or base station which is referred to as a Central Network Entity. When it comes for CRAHN there will be no central access point for monitoring the traffic, but the nodes will communicate with one another in both Licensed and Unlicensed spectrum bands. Radio spectrum is a key characteristic of CRAHN as it will first come into significance when any new user wanted to join the network. The new node will monitor the availability of all spectrum in a given cluster and when it feels that the spectrum was unused for a significant amount of time then it will take over that unused spectrum and will start transmitting data and communicating with the other nodes in that cluster. For illustration the architecture of CRAHN is shown in Fig. 1 which demonstrates the differences between Primary network and CR network [6]. Another difference between the two modes of operation is that CR users can utilize both licensed and unlicensed bands whereas in CRAHN the visiting nodes can access only licensed bands which is reserved for PU's of that network making the communication reliable and with no interference. But at times the PU's need to share and communicate data arising from unlicensed spectrum bands although they operate only on licensed bands based on the local observations of the network and the nodes. Cognitive Radio Ad hoc Network consists of three types of Routing Structures. They are a) single radio multi-channels, b) equal number radios and channels and c) multi-radios multi-channels.

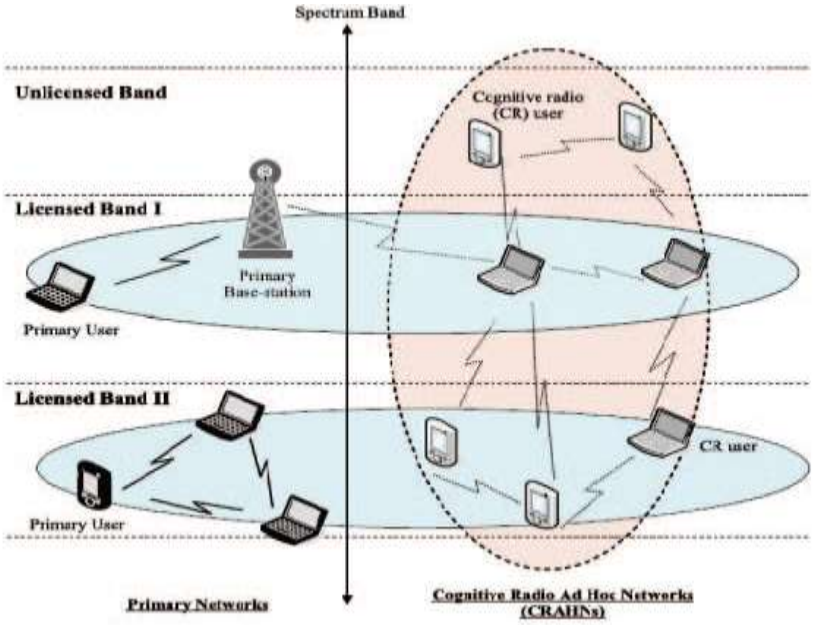

Figure 1: CRAHN architecture [6]

Routing Protocols

Routing is defined as a mechanism for transmitting data from source node to destination node with the help of intermediate nodes and addresses issues of hop count, minimum delay and congestion. In Ad hoc Networks the routing is classified into three broad categories Proactive Routing, Reactive Routing and Hybrid Routing [7]. In Proactive Routing each and every node will update with fresh lists of destinations along the routes to that node by periodically distributing the routing table among the network. In Reactive routing the entire network will be flooded with route request packets to find the best route to the destination. In Hybrid Routing this combines the advantages of Reactive and proactive and will route the packets. In the above discussed protocols there are many protocols have been implemented like CR-AODV[8], DSR-MR[9] ,WCETT[10], MR-AODV[11], RACARP, SEARCH,CRP, CCODRP, ROPCORN[12], ARAN[13].

As stated above with the types of Routing protocols in CRN's the main interest was laid for in On-Demand routing protocols, where the routes are created only when it is necessary to establish it between any pair of nodes in a network topology. We have clearly examined about AODV and this protocol was designed on three standard principles

a) When any SU(Non Local User) wants to establish any connection with the cluster then it should not interfere in the PU's Spectrum b) It tries to minimize the route cost by applying a joint path and best channel selection. c) It also tries to improve the overall performance with the help of multi-channel selection. So far many extensions of AODV are proposed like CR-AODV, MR-AODV, AOMDV and DSR, DSDV [14], and many simulation studies were carried out on various size of inputs and Radio Channels.

CR-AODV

CR-AODV is a protocol that calculates the route between the any nodes on demand that is it will compute the route when there is some data to transmit. For this process to carry out it involves four messages that will be involved using CR-AODV nodes. The messages are route request (RREQ), route reply (RREP), route error (RERR) and HELLO messages [14]. Each message has a specific meaning designated for it. RREQ is used to perform route discovery between the source to destination. This route will not be fixed and if after a period of time if the source node wants to transmit any packet to the destination then again the same process will be carried out. This is analogous to the concept when a node receives a RREQ control packet it examines whether it is a fresh request or an existing request that was arrived in the process of broadcasting. If it is new then the RREP will be sent to the destination else it employs a reverse path to find if there is any other path to the source node. Once after this process gets completed then RREP control message is sent to inform the creation of the new nodes for message transmission. HELLO messages are only used to broadcast the information of the neighbors in the network. RERR is used to initiate the route discovery if still there is need for the route. CR-AODV routing process will be carried out in a way that if there is any data to be transmitted between source to destination then it senses for the availability of the channel. If the route is available then the packet will be transmitted else the packet will be saved in the local queue and later on again the RREQ must be initiated for route establishment. This is as shown in Fig 2.

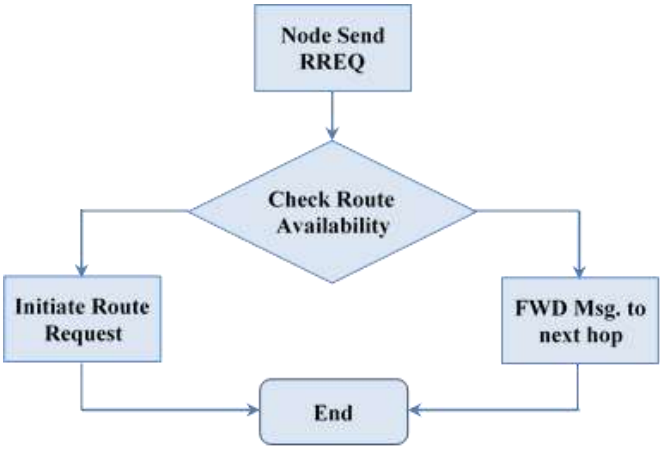

Figure 2: CR-AODV protocol

Limitation of CR-AODV

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-III and RSA-32 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 CRAHN, 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. But in none of the above stated protocols there is no security provided and some of them has proposed with few security parameters but not in complete. Here in our paper we have proposed a hybrid CR-AODV protocol by using RSA-32 and SHA-III for security and integrity. We have simulated the work and compared the results and examined that the performance was more with slight delay. If security is a concern then our work will address the issue. The rest of the paper is organized as follows 2. Related Work 3. Proposed Work 4. Simulation and Results.

Related Work

In [15], the primary focus that was proposed was to take care of secondary users who actually try to access the channel in a cognitive radio ad hoc network who can be selfish users/ nodes and malicious users/ nodes for which security feature needs to be adapted. In this process when nodes enter the network it will be very much needed to provide to the network as the new nodes commonly referred to as Secondary Nodes try to gain access to the network by initializing the process of route discovery and route maintenance, which was given by a metric called as trust value in CRAODV-S.

The research on CRAODV-S for establishing an efficient routing discovery process was carried out on the subsets of trusted channel which was again compared with the original CR-AODV [16][17] . In general discovery process of identifying the route from a source node to the destination node the source node will initiate certain control packets and in turn the remaining set of active nodes will also respond to these control packets being RREQ,RREP, SU_RREQ, SU_RREP, HELLO and RERR which are operated in a similar manner along with one more control packet PU_RERR was implemented when the primary user senses there is no such node in existence along with the proper utilization of the spectrum was discussed. There is quite a significant role for each control packet the primary being the RREQ which will flood the entire cluster to find the path to the destination during the route discovery phase.

In Conventional CRAHN the RREQ message will be continuously moving within the network until it will reach to the intended destination. Although the process that was stated seems to be simple there are some underlying constraints that needs to be addressed like upto when should be this control packet be broadcasted and when should it be dropped. This issue was addressed as every control packet that gets transmitted will have a limit on hop count as how many steps it can take and TTL field which specifies the Time To Live for a specific message. The process will be continued until it reaches the destination node and when the destination node commonly referred to as sink node was identified then the RREP packet will be acknowledged in the reverse direction and all intermediate nodes will update this entry in their routing tables.

Another issue that was addressed during this process was that when any intermediate node along this reverse path of RREP examines that this node/activity is interfering the activities of the PU then it can immediately drop the control packet RREP otherwise the same activity is repeated. Another important characteristic of this approach was that instead of the intermediate nodes sensing the channel for any PU activity the SU may transmit a SU_RREP to the source node using the same channel through which the control packets are received. It will check for any duplicate packets and discard it if it was found as maintaining a number of routes will be an overhead for any intermediate node.

During the route discovery process there may a chance of Black Hole attack or grayhole attack or selfish attack if there is any malicious node available in that network. In order to overcome these attacks the trust value comes into significance that will be assigned to every secondary user in a network. This value is generally computed using threshold values of the lower bound time value of the route reply message packet. If this trust value is lower than the lower bound value of threshold then it will be treated as a malicious secondary node which possibly leads to blackhole attack. In this blackhole attack the malicious nodes will start to transmit false messages. Whenever any malicious nodes receives this control packet then it immediately acknowledges with a high sequence number in an attempt to make an entry into the SU routing table. Before this SU identifies that this node was a malicious node as it may receive acknowledgements from remaining nodes regarding the activities of PU it may transmit packets which will be dropped by remaining or this malicious node. This is the process how the malicious nodes act as selfish nodes and take control over the network and will be jamming all the messages and will always keep the PU's channel being free from any SU activities in CRAHN.

In the existing model the channel if free will be accessed only when it is required. The malicious nodes will also be active at the initial time during route request and when the SU records this entry it its routing table and starts transmitting packets then the malicious node will launch a Denial of Service attack. The SU will not simply updates its routing table as there can be a chance of DOS attack and hence it will be taking decisions based on the trusted value. This is normally done when it senses that SU_RREP message was secure and the route was better using the same channel. Another key aspect that needs to taken care in CRAHN is Route Maintenance process. There are two classifications in this one being the RERR which mainly needs to be addressed as the topology of the ad hoc network is dynamic, and other being PU-RERR for handling the activities of the PU. This PU-RERR will be acting as a control message to identify all SU nodes within a network to see if any of them are accessing the channel of PU and if it was found then simply the node will be discarded from the routing table.

When any SU receives PU-RERR control packet then they have to nullify the currently using channel as it may be interfering with the activities of the PU. This will also not allow new routes or new nodes in the channel. When any node in the network identifies that the channel is free it will again

reevaluate the entries and the same process is carried out. This is how they have implemented Route Discovery and Route Maintenance and have evaluated the performance of their protocols against various parameters like throughput, packet delivery ratio, and end-to-end delay and normalized routing load and showed that their model performed well.
The main limitation of the existing model was that the proposed security model was based on trust values and the trust value is given based on the SU's activities. When any new node joins the cluster it was just given a moderate trust value, but based on this value if it was given access to the spectrum then there is a chance for it to be a suspicious node. So this was not a better choice as well as there is no way to authenticate message at the receiver end. These issues were addressed in our proposed model.

Proposed Work

The work was proposed mainly to issue a primary concern in any Ad hoc Environment being Security In CRAHN the topology was not fixed as any number of users can simply join and leave the network and for proposing and verifying the authenticity and malicious behavior may not possible at all times. There is a way how we can add security to the present infrastructure without effecting the remaining parameters. This work that was developed and implemented guarantees a secure communication using most powerful security algorithms by using RSA-32[18] bit Crypto-System and Digital Signature using SHA-3[19].The main striking balance for going with the above two mechanisms was that Ad hoc Network by nature is light weighted which works with fewer resources providing efficient results. The entire process of communicating in any network starts with the Route Discovery process. In this communication we can communicate in a secure manner with low range radio signals and the nodes that participate in this communication will not be aware of how this actual system of security features will perform.
The process that was carried out is very simple and the security schemes discussed were clear and will be evaluated in default mode. The authentication of this service is implemented using Digital Signature SHA-III and confidentiality is served based on RSA-32 cryptosystem. As the initial step to verify the results the source node first tries to locate where the destination node is available to transmit the data or control packet. But in general during the Route Discovery phase there will be a need to know the route to the destination which is done by transmitting the RREQ message to its immediate neighbor using the destination id. When any intermediate receives this message it check three conditions whether the destination node was it or not then it can simply read the message. The second criteria it will check is whether it belongs to that group. If this is also not true then it simply forwards the packet to all its destinations. Once it reaches the destination then the route will be established between source to destination and it also will separate the type of data being carried. The message that any nodes receives will consists of information where that information can be Mutable or Non Mutable. Mutable information is information that can be modified and this in general consists of Hop Count or TTL as the value needs to be updated frequently. In the case of Non Mutable Information this consists of the destination node's digitally signed document that will be sent along RREP packet. Now the actual process of Route Discovery starts whenever any new node enters then it will check the digitally signature and if it matches then only the packet is forwarded or else then it is simply dropped. Now the reverse process of RREP will be acknowledged and in any case if the first id of the source was not matched then it will be discarded by the Source itself.
After successful establishment of route and signed information at each intermediate node the source will select a random key for the intermediate nodes to transmit the packet to the destination. The key can be gathered from the trusted neighbor or from the digital signature. The sender will encrypt the message with RSA and the destination will do the reverse process of decryption. After successful decryption of message at the receiver and verifying the integrity of the message the receiver will acknowledge back to the sender. The source will only confirm about the successful complete cycle of transmission once it receives an acknowledgement. If the acknowledgement was not received to the sender then again the same message will be retransmitted in a different route. This process of work that was carried out is an enhanced version of AODV that still will maintain shorter routes to destinations and also will lower the end-to-end delay and helps in longer battery life compared to the existing models. The detailed working is shown in Figure 3.

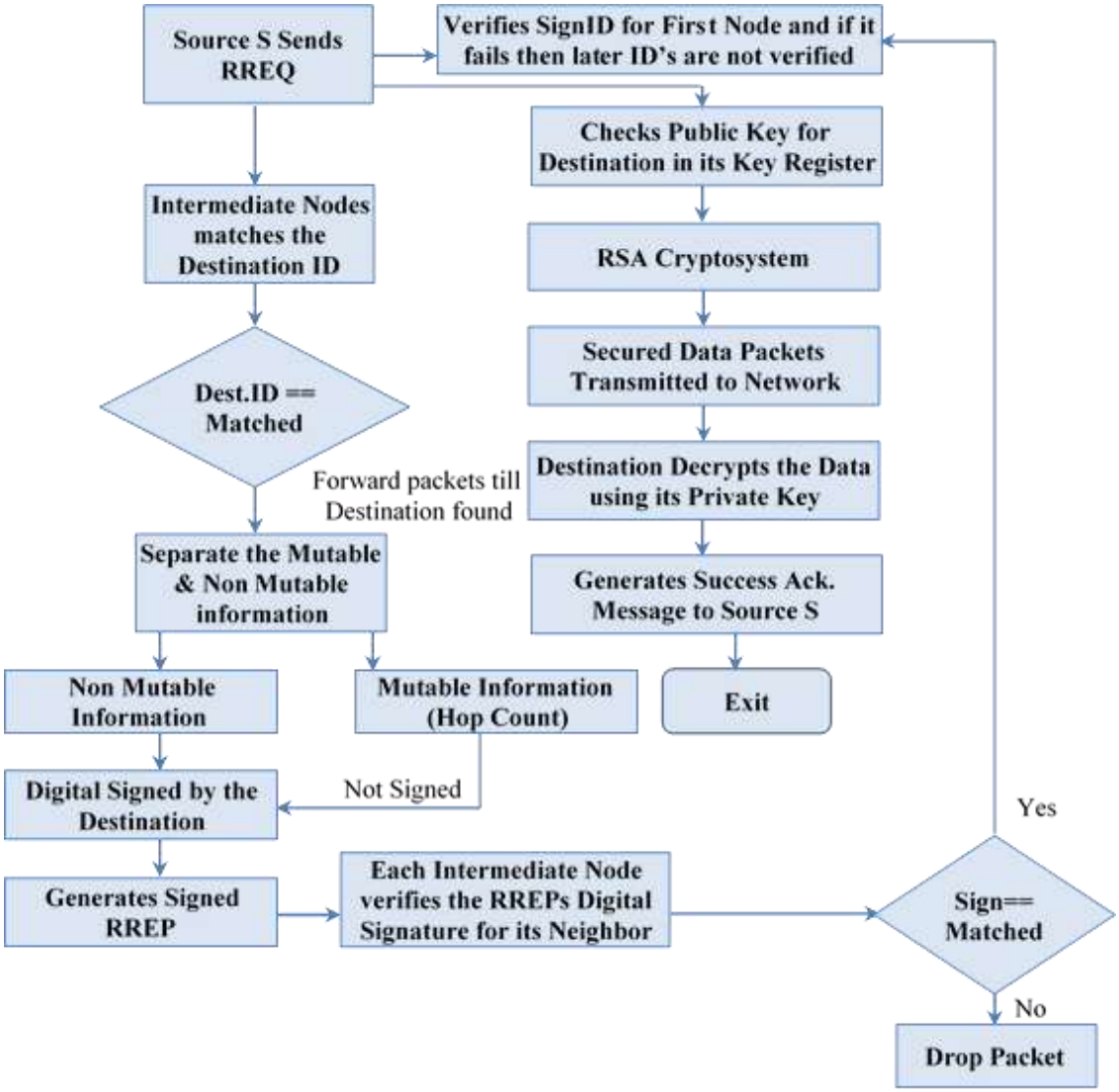

Figure 3: Flow chart for proposed system (CSR-AODV)

Results And Discussion

In this proposed research work, three kind of CR routing structures are presented: 1) Single- radio, multi-channels, 2) equal-radios, equal-channels and 3) multi-radios, multi-channels. For simulating the experiment scenarios, the network simulator used is NS2 along with Cognitive Radio Cognitive Network (CRCN) patch. For creating the environment we have taken the rich set of functions from TCL library, which helps in creation of several copies of Link Layer, queue for storing messages, Media Access Control , Network Interface Card and channels for each individual radio in C++ library. The simulation parameters are in detailed provided in Table 1. The performance of CSR-AODV and CRAODV-S are examined and compared using multiple random topologies. Table 2 shows the comparision of CRAODV-S(Existed) and CSR-AODV(Proposed) in different parameters.

Table 1: Simulation Parameters

Parameter	Values
Topology	1000 X 1000 m^2
Traffic type	FTP
Packet size	512 bytes
Simulation duration	50 seconds
Transport layer	TCP

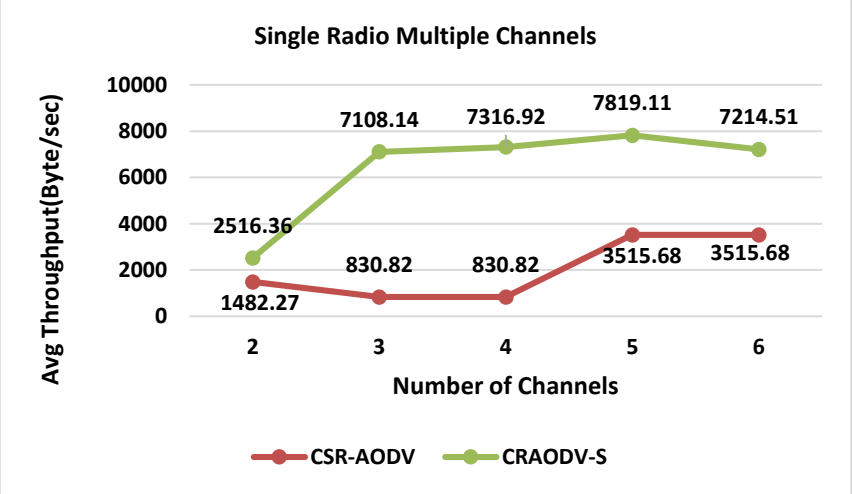

Figure 4: Result for single radio and multi-channels for CSR-AODV and CRAODV-S

Fig 4. shows the overall throughput gathered majorly will be changed when the number of channels increases. As we discussed about the scenarios during the development phase, the simulation results for each scenario is analyzed. CRAODV-S routing protocol gathered higher average throughput in scenario 1 which is 7819.11. Meanwhile, in CSR-AODV routing showed lower average throughput in scenario 1 which is 3515.68. CRAODV-S routing protocol has a significant average throughput in scenario 1 where the average throughput is 214% higher than CSR-AODV routing protocol. But this result significantly varies when we change the number of channels and radios proportionately.

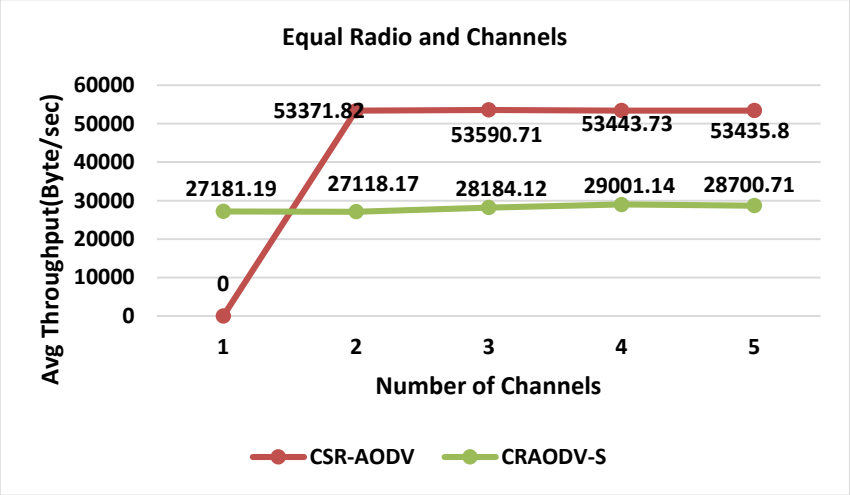

Figure 5: Result for equal radios and channels for CSR-AODV and CRAODV-S

Fig 5. shows the overall throughput gathered majorly will be changed when the number of channels increases. As we discussed about the scenarios during the development phase, the simulation results for each scenario is analysed. CSR-AODV routing protocol gathered higher average throughput in scenario 2 which is 53590.71. Meanwhile, in CRAODV-S routing showed lower average throughput in scenario 2 which is 29001.14. CSR-AODV routing protocol has a significant average throughput in scenario 2 where the average throughput is 84% higher than CRAODV-S routing protocol.

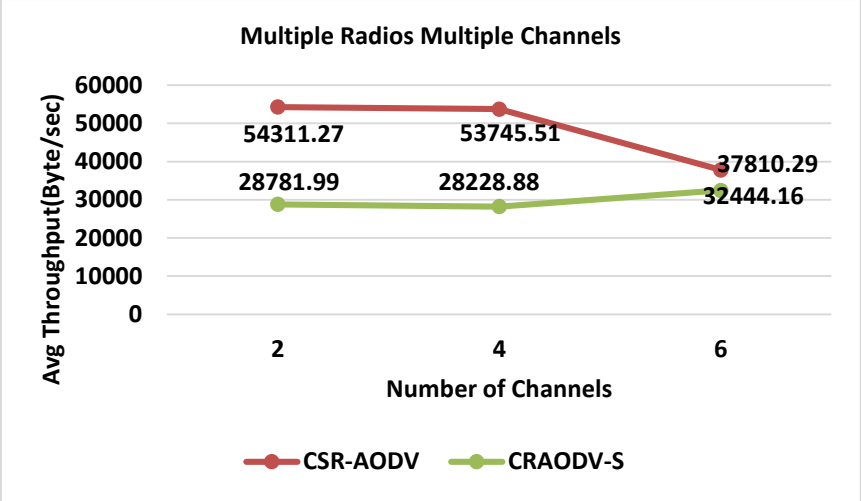

Figure 6: Result for multi-radios and multi-channels for CSR-AODV and CRAODV-S

Fig 6. shows the overall throughput gathered majorly will be changed when the number of channels increases. As we discussed about the scenarios during the development phase, the simulation results for each scenario is analysed. CSR-AODV routing protocol gathered higher average throughput in scenario 3 which is 54311.27. Meanwhile, in CRAODV-S routing showed lower average throughput in scenario 3 which is 32444.16. CSR-AODV routing protocol has a significant average throughput in scenario 3 where the average throughput is 67% higher than CRAODV-S routing protocol.

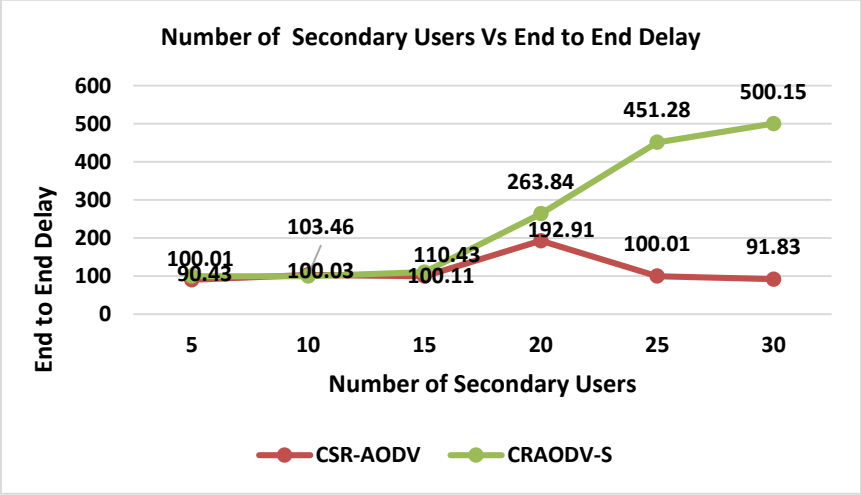

Figure 7: End to end delay vs number of secondary users

As shown in Fig 7 it was clearly observed that End to End Delay for CSR-AODV was less compared to CRAODV-S. As the number of Secondary Users who are accessing the network increases our proposed model was able to handle it in an effiient manner. At one stage when the number of SU's are 20 there is a significant increase in delay and again as the number of users increased we can see the decrease in delay. The average End to End Delay for CRAODV-S is more i.e, 255.36 ms compared with that of CSR-AODV which is 112.68 ms.

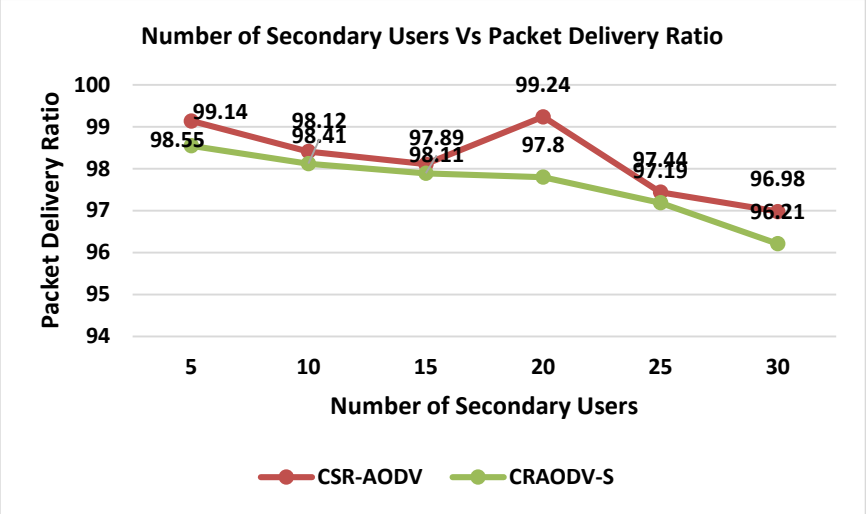

Figure 8: Packet delivery ratio vs number of secondary users

As shown in Fig 8 it was clearly observed that Packet Delivery Ratio for CSR-AODV was more compared to CRAODV-S. As the number of Secondary Users who are accessing the network increases our proposed model was able to handle it in an efficient manner. At one stage when the number of SU's are 20 there is an increase in this component and again as the number of users increased we can see a slight decrease in Delivery compared to the peak value. The average Packet Delivery Ratio for CSR-AODV is more i.e, 98.18 compared with that of CRAODV-S which is 97.71.

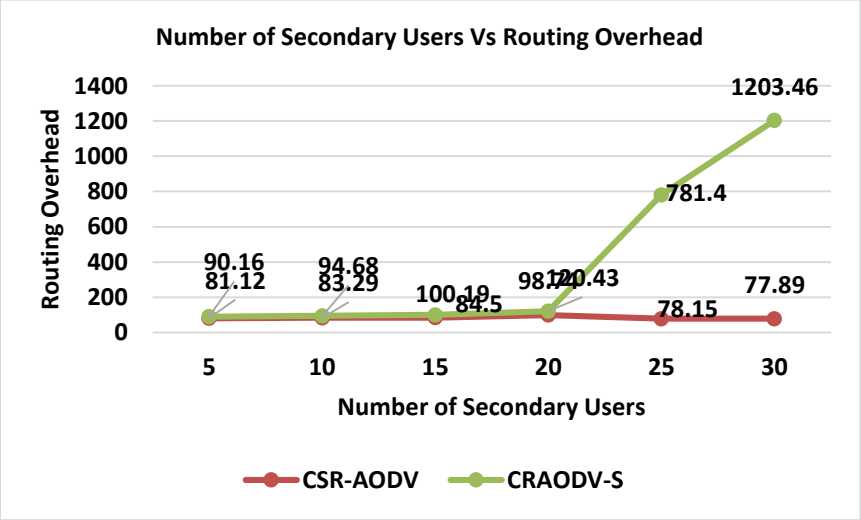

Figure 9: Routing overhead vs number of secondary users

As shown in Fig 9 it was clearly observed that Routing Overhead for CSR-AODV was less compared to CRAODV-S. As the number of Secondary Users who are accessing the network increases our proposed model was able to handle it in an effiient manner. At every stage when the number of SU's are increasing there is no significant change in Routing Overhead. The Average Routing Overhead for CRAODV-S is more i.e, 393.38 compared with that of CSR-AODV which is 83.94.

Table 2: Performance comparision of CRAODV-S(Existed) and CSR-AODV(Proposed)

Sno	Parameter	CRAODV-S (Existed)	CSR-AODV (Proposed)
1	Higher Average Throughput in Single Radio multiple channels	7819.11	3515.68
2	Higher Average Throughput in Equal Radios and channels	29001.14	**53590.71**
3	Higher Average Throughput in Multi Radios and multi channels	32444.16	**54311.27**
4	Average Throughput in Single Radio multiple channels	314%	100%
5	Average Throughput in Equal Radios and channels	100%	**184%**
6	Average Throughput in Multi Radios and multi channels	100%	**167%**
7	End-to-End Delay	255.36ms	**112.68ms**
8	Packet Delivery Ratio	97.71	**98.18**
9	Routing Overhead	393.38	**83.94**

Conclusion

The proposed project met with the objectives, that was to investigate and compare the network performances of CSR-AODV and CRAODV-S routing protocols in CRAHN and analyze performance based on the parameters of average throughput, end to end delay, packet delivery ratio and finally routing overhead. To evaluate the above stated performances we have implemented them in 3 types of routing structures, the structures that are considered are single radio link consisting of multiple channels, equal number of radio links and channels and multi-radio links with multiple channels. After thorough experimentation on the discussed models and performance parameters, data was collected and observed. Based on the results of experimentation we can conclude that CRAODV-S routing protocol was proved to be more efficient for implementing in single radio link and multiple channels structure. The performance improvement was due to increase in optimal total average throughput. CSR-AODV routing protocol was proved to be more efficient for implementation in the remaining two routing structures compared to CRAODV-S.

References

[1] Mitola, J. and Maguire, G.Q., 1999. Cognitive radio: making software radios more personal. *In IEEE personal communications*,Vol.6, No.4, pp. 13-18.

[2] Jovicic, A. and Viswanath, P., 2009. Cognitive radio: An information-theoretic perspective. *In IEEE Transactions on Information Theory*, Vol.55, No.9, pp. 3945-3958.

[3]Yu, R. et al, 2012. Secondary users cooperation in cognitive radio networks: balancing sensing accuracy and efficiency. *In IEEE Wireless Communications*, Vol.19, No.2, pp. 30-37

[4]Girish, V. et al, 2009. Design issues in wide scanning range cognitive radios. *In Cognitive Wireless Systems (UKIWCWS), First UK-India International Workshop, IEEE*. New Delhi, India, pp.1-5.

[5]Ejaz, W. et al, 2011. Fully distributed cooperative spectrum sensing for cognitive radio ad hoc networks. *In Frontiers of Information Technology (FIT), IEEE*. Islamabad, Pakistan, pp. 9-13.

[6]Akyildiz, I.F. et al, 2009.CRAHNs: Cognitive radio ad hoc networks. *In AD hoc networks*, Vol.7, No.5, pp. 810-836.

[7]Kaur, R. and Rai, M.K., 2012. A Novel Review on Routing Protocols in MANETs. *In Under-graduate Academic Research Journal (UARJ)*, Vol.1, No.1, pp. 103-108.

[8]Chehata, A. et al, 2011. An On-Demand Routing Protocol for Multi-Hop Multi-Radio Multi-Channel Cognitive Radio Networks. *In The International Conference on Wireless Days (WD), IFIP, IEEE.* Niagara Falls, ON, Canada, pp. 1–5.

[9]Biaz, S, et al, 2007. Evaluation of Multi-Radio Extensions to DSR for Wireless Multi-Hop Networks. *In International Conference on Wireless Information Networks and Systems (WINSYS'07)*. Barcelona, Spain, pp. 65-69.

[10]Draves, R. et al, 2004. Routing in multi-radio, multi-hop wireless mesh networks. *In Proceedings of the 10th annual international conference on Mobile computing and networking, ACM*. Philadelphia, PA, USA, pp. 114-128.

[11]Pirzada, A.A.et al, 2006. Evaluation of multi-radio extensions to AODV for wireless mesh networks. *In Proceedings of the 4th ACM international workshop*

on Mobility management and wireless access, ACM. Terromolinos, Spain, pp. 45-51.

[12]Talay, A.C. and Altilar, D.T., 2009. ROPCORN: Routing protocol for cognitive radio ad hoc networks. *In Ultra Modern Telecommunications & Workshops, ICUMT. International Conference, IEEE*. St. Petersburg, Russia, pp. 1-6.

[13]Sanzgiri, K.et al, 2002. A secure routing protocol for ad hoc networks. *In Network Protocols, Proceedings 10th IEEE International Conference, IEEE*. Paris, France, pp. 78-87.

[14]Singhroy, S.H.R.U.T.I.et al, 2013. Comparative Analysis of AOMDV, AODV, DSR and DSDV Routing Protocols for Cognitive Radio. *In International Journal of Electronics, Communication & Instrumentation Engineering Research and Development*, Vol.3, No.1, pp. 1-6.

[15]Sethi, S. and Pal, S., 2015. CRAODV-S: A Secure On-Demand Routing Protocol in Cognitive Radio Ad Hoc Network. *In International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)*, Vol.14, No.2, pp. 103-109.

[16]Pal, S. and Sethi, S., 2015. Selection of Reliable Channel by CRAODV-RC Routing Protocol in Cognitive Radio Ad Hoc Network. *In Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI, Springer International Publishing*, Vol. 2, Hyderabad, Telangana, India, pp. 251-259.

[17]Sethi, S. and Pal, S., 2013. Effective routing protocol in cognitive radio ad hoc network using fuzzy-based reliable communication neighbor node selection. *In Proceedings of the International Conference on Frontiers of Intelligent Computing. Theory and Applications . Springer, Cham,* Bhubaneswar, Odisha, India, pp. 17-24.

[18]Dian, K.et al, 2017. RSA 32-bit Implementation Technique. *In International Journal of Recent Trends in Engineering & Research (IJRTER),*Vol.03, No.7, pp. 279-284.

[19]Bertoni, G.et al, 2011. The Keccak SHA-3 Submission version 3. *Submission to NIST (Round 3)*, pp. 1-14.

