Performance Analysis of Cross-layer Efficient Selfishness Prevention Routing Protocol for the Dynamic CR Networks

R. Sri Uma Suseela, KSN Murthy, Hima Bindu Valiveti

Abstract*: *As wireless communication is very dependent on the use of spectrum, increased demand for and practical application of new wireless services generally leads to spectrum shortages. A remarkable feature of protocols in the cognitive radio is to, to detect the selfish behaviour of node and discard the abnormal packets. However, minimize transmission latency and enhance energy efficiency are two main issues in multi-hop Cognitive Radio Networks (CRN) where it is difficult to gain knowledge of topology and spectrum statistics. The misconduct of selfish nodes such as not participating in the routing process, delaying RREQ packet intentionally, removing the data packet, not responding or sending hello messages. This misconduct of the selfish nodes will affect efficiency, trustworthiness, and fairness. This paper proposes the cognitive radio dynamic nature, associate with that of selfish nodes, the cross-layer efficient Selfish Prevention Routing Protocol (ESPRP). All the above characteristics are simulated with help of NS-2.35 simulator, and our proposed protocol attains good enactment in terms of lower delays, higher throughput and better packet delivery ratios for collaborative node traffic related to traditional routing protocols in the cognitive radio.

Index Terms*: Cognitive radio, *Selfish attack, Decentralized Trust Model, Layer Modelling, and routing protocol

I. INTRODUCTION

Cognitive radio (CR) is an analytical radio under which the commensurate communication system, for instance in the field of RF positioning and use, has its knowledge internally and externally [1]. It can decide on working behavior using this data against prearranged objectives. A CR regularly reviews its performance and interprets its results, then uses this data to analyze radio backgrounds, channel state information, throughput, and more, then modifies its radio parameters to meet the required QoS restrictions, operational constraints and administrative constraints [2]. The growing market for wireless networks tends to increase security difficulties. However, it is susceptible to most security threats due to the complexity and critical applications of the cognitive radio network [3, 4].

Despite this great advantage, guaranteeing security for these networks is a major challenge. According to observations, CRN has a group of little vulnerability that cannot easily be rectified. To resolve such threats, CR should probably learn to be environmentally aware. Since the CRN is resilient to most attacks, there are very few attacks that can severely affect the CRN. The primary objective of CRN safety is to safeguard primary users and their range while competing for resources with secondary unlicensed users. In cognitive radio networks, there are three types of selfish attacks. In cognitive radio networks, there are three different types of selfish attacks. They are signals for fake selfish attacks, the signal for false selfish attacks and a selfish attack by dynamic access behavior.

In this paper, we immediately identify several selfish nodes in the egoistic attack of channel pre-occupation. In this attack, a selfish cognitive radio node is attempting to occupy the primary spectrum resources completely or partially available. The selfish nodes will degrade network performance substantially. Selfish attacks can take place in the communication environment that is used to transmit the currently available channel information to nearby transmission nodes. Hence why the major concern is when and how often the attacker and CR system defender should carry out both the PUE selfish assault and the channel surveillance process.

Recent protocol developments in the cognitive network seem to be a major issue because of the unavailability of centralized regulation have led to selfish nodes in the network. There is a need for cross-layer for efficient prevention in the network that can have the ability to reduce selfishness in the routing protocol to make the cognitive radio to be more dynamic in all the cases. The conducted workouts clearly show that by increasing the throughput, lower delays and better delivery ratio, SAR offers better performance. It can, therefore, be said that cross-layer selfishness avoids the routing protocol.

The main contributions and organization of this paper are summarized as follows: In section 2 we describe background details of attacks in CR network. Section 3 discusses the proposed work. Section 4 deliberates results and discussions. Finally, in section 5, we concluded the paper.

II. BACKGROUND WORKS

In [5], an attack on the physical layer was submitted by the authors. The authenticated users are facing severe problems with the attackers as they attack the packets that are intended for the authenticate users during the transmission session. The attackers also make the radio transmission interference by sending damaged packets to the user. In [6], the authors discussed how the attacker behaves selfishness by sending false sensing data to its all neighbouring nodes and the fusion center that results in Spectrum Sensing Data Falsification (SSDF), the attack induces a recipient to make an incorrect spectrum-sensing decision. This attack targets centralized as well as distributed CRNs.

Revised Manuscript Received on July 22, 2019.

R. Sri Uma Suseela, Research Scholar, Department of ECE, KLEF, Vijayawada, Andhra Pradesh, India
Dr. KSN Murthy, Professor, Department of ECE, KLEF, Vijayawada, Andhra Pradesh, India
Dr. Hima Bindu Valiveti, Professor, Department of ECE, GRIET, Hyderabad, Telangana, India

In [7, 8], attacks in the link-layer were discussed in authors. Cognitive radio can refuse to transfer data to a different host in a multi-hop cognitive radio network. This leads to energy conservation and increased output and even worsens the total CRN. So, to detect the efficiency of detection time the probability test is conducted. Network layers of attacks include sinkhole attacks and HELLO flood attacks. The Sinkhole attack turns out to be the best way to reach a particular destination and attract neighbouring nodes to use it for forwarding their packets. This is the reasonable way an attacker can carry out a new attack to be coined to be selective forwarding technique, in which the packets can be supposed to be modified or discarded from the network's node. Infrastructure and mesh architecture, such an attack is effective because all traffic moving across the network fusion center, having the ability of an attacker to select the best router for forwarding all the packets through it.

A. Modelling of layers

In practice, to give information regarding different layers, there is a need for considering the multi-hop network with dynamic characteristics for N number of nodes. It contains an adaptive power control rate (PCRA) system with the MAC layer support almost 12 wireless channels that non-overlap with the IEEE 802.11a/g for channel duration of t_d ms.

B. Behaviour of the node

In this work carried out from [9], the nodes are assumed not to be malicious, to interfere with other neighbour nodes in the network through the transmission of fake information or interference in the transmission of others. But the nodes can be selfish in their conduct. Depending on the selection of argument *sf*, the node behaviour can be decided. Using the relationship sf=0 the node is ready to transmit packets to other nodes in the network, in a similar manner when sf=1 node cannot transmit packets.

C. Modelling spectrum opportunities

The accessibility of the irregular channel can be characterized by three parameters premised on an inter-weave model: the primary one is to find the primary user (PU) probability p of sending to the secondary user (SU), the secondary is to get the idle state duration i and final one is to get the busy states mean duration b. So by these views, it is clear that states of the channel are switching concerning accessibility and inaccessibility periods following p, i and b.

D. Decentralized Trust Model

We use the most widely used algorithm [10] to impose security as well as to prevent selfish behavior to determine the detect each and every node in the network in regualr manner. A public and a private key pair are involved in RSA. Everyone can know the public key and use it to encrypt messages. Only private key can decrypt messages encrypted with a public key. In the key generation process, it is supposed to use two keys are generated, the primary is the public key $P(n,e)$ and secondary is private key (d). To obtain the value of the trust of every node in the network, it is required to collect the information about collaboration index (CI) present in the neighboring nodes. The purpose of updating the value of CI is responsible for listening to the original or control information with the help of neighbor nodes.

III. SYSTEM MODEL

The ESPRP aims to choose the best course keeping in mind the reputation of nodes, SOPs and delays. In two network layers, we use a cross-layer methodology to resolve issue of network:

(1) MAC Layer–Key Generation, Secure Join Request, Secure RTS / CTS, Identity authentication and Transmission Control.

(2) Layer Network–Route Discovery, Selection of Route and Optional Route.

The ESPRP arrangement is useful largely because it maintains secure MAC address and independent routing as illustrated in figure.2 that can possess several tasks.

The secure framework primary purpose is to ensure nodes identification that makes data and control information exchanging with the MAC module. Another purpose of the proposed protocol is that it helps to pick the best route from a source node to a destination node by exchanging route requests and route reply packages. During the actual routing, a transmission power control (TPC) and opportunistic routing (OR) are being responsible for decreasing the failed delivery rate.

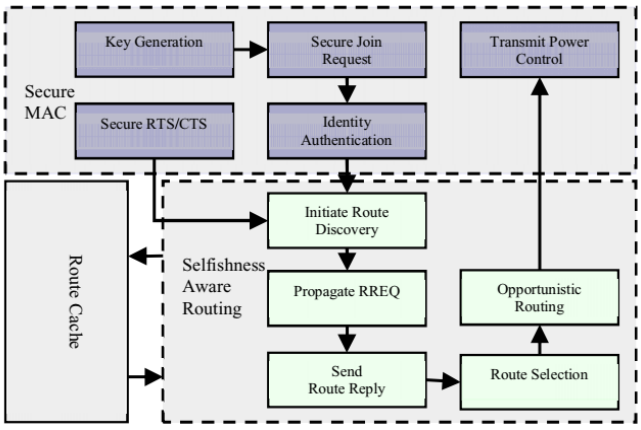

Fig.1. ESPRP Flow Diagram

A. Secure Join Request

In the request joining phase the node that supposed to join the cognitive network starts broadcasting the Request to Join (RTJ) packet through control channel to the request node m. As this node with its MAC address and Secure Hash Algorithm (SHA-1) can explicitly states as mod d SM n. Therefore the requested node have the public key (n, e) and the requested node MAC Digest S sent control channel in the given CRN.

B. Identity Authentication

A sponsor node is called that enables the soliciting node to enter the CRN for the purpose of collecting required RTJ, then supposed to use the SHA-1 together with the MAC address of the soliciting node in order to calculate M. The operation $M'=S^e \bmod n$ is performed and the digest M' is compared to the actual M digest of the message.

C. Route Discovery

In general the SPRP, discovering of route is somewhat similar to dynamic source routing (DSR) technique. In this protocol, route identification of any random cognitive radio network destination begins with the sending of RREQ packets. When another destination node obtains a

RREQ packet, a copy of the collected route record from the RREQ packet is produced by Route Reply or RREP.

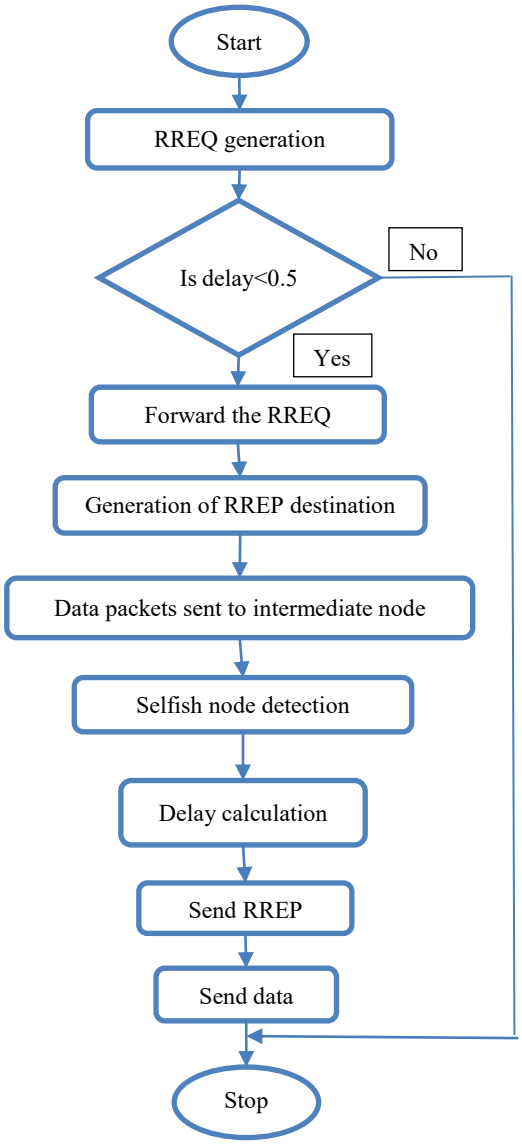

Fig.2. Flow chart

D. Operation

Figure. 2 shows that if any node has data packets that simply send the node first checks to make sure whether or not there are routes to the destination in the route cache. If routes are already present, the packets on those other paths are sent. Unless routes are not present, it floods all its neighbouring nodes with the RREQ message. If any intermediate node receives RREQ message, then it first needs to check if the destination route is recognized if the RREQ packet is generated. We can search a node in the routing table using the final node. When the RREQ value reaches the destination, the incoming paths are put in the cache along with the RREQ packet. RREP is generated and it must update its value if the node is part of RREP. When a selfish node receives RREQ, it increases the times of receipt, significantly increases the time of reception by 0.2seconds, and increases the number of messages by 3.

IV. RESULTS AND DISCUSSION

The simulation studies were conducted using NS-2.35 package to evaluate the performance of the proposed ESPRP system. We simply consider a network topology of 60 nodes covering 3 PRNs. The nodes are divided into 3 groups of 18 nodes. 1/3 of each PRN is continuously unselfish (*sf*=0), 1/3 is selfish (*sf*=1) and the remaining is egoistic with a probability of s and altruistic with a probability of 1-*s* (*sf*=*s*). The nodes in each group are clustered completely randomly within a circular area of 1000m. There are three circular regions and the centre of each region is 1500 meters apart.

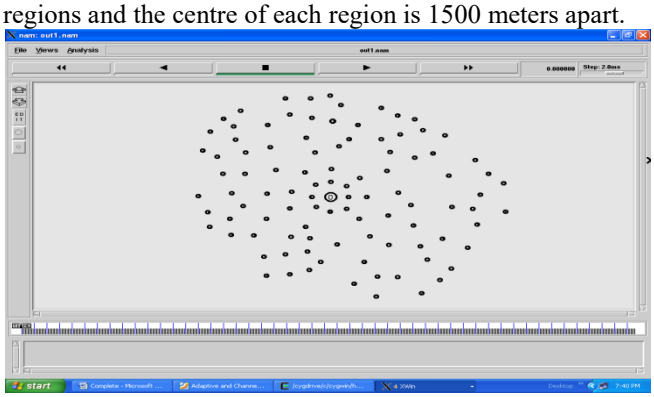

Fig. 3.Initial set up of the CR network

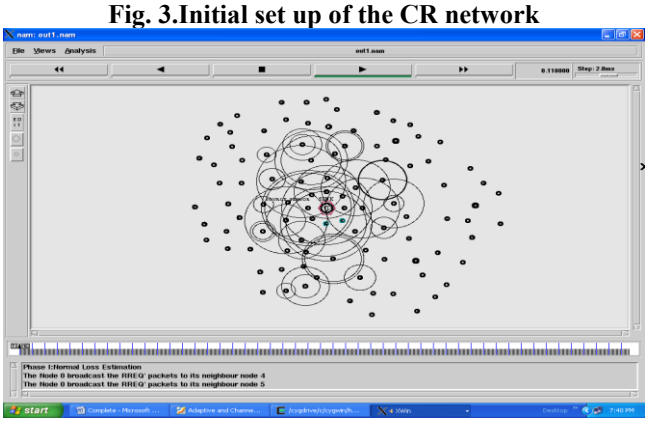

Fig. 4.Nodes deployment

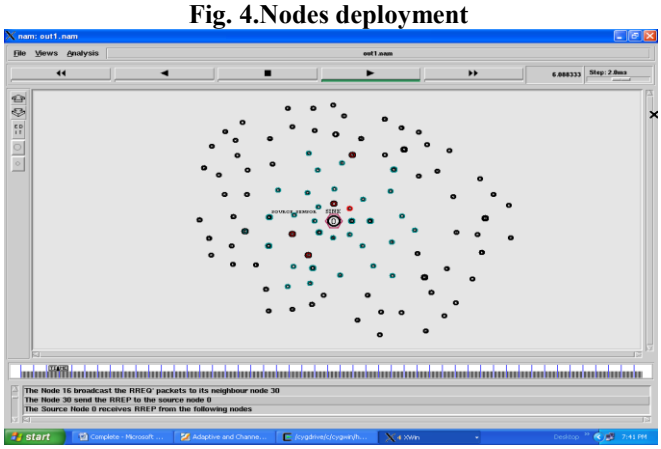

Fig. 5. Node movement

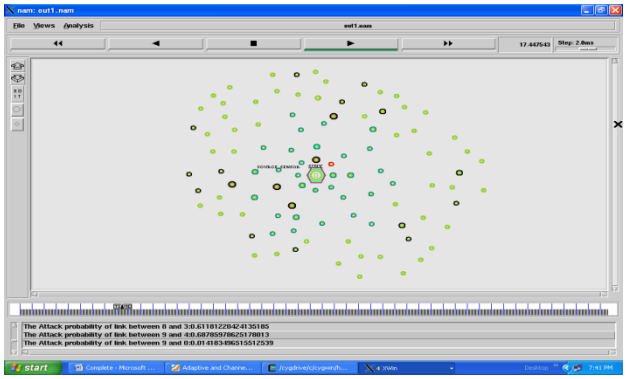

Fig. 6. Selfish Node attack

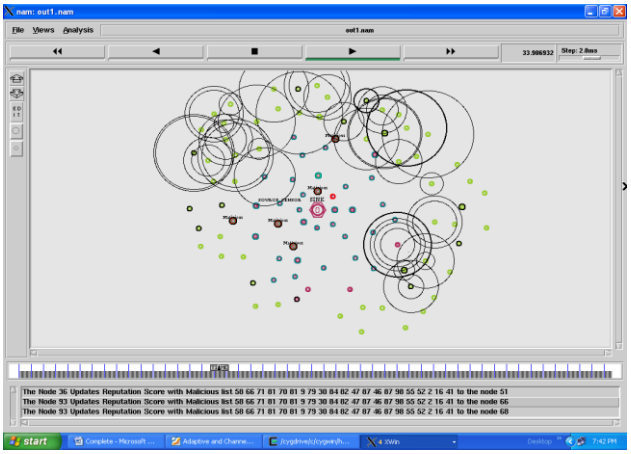

Fig. 7. Selfish Node attack

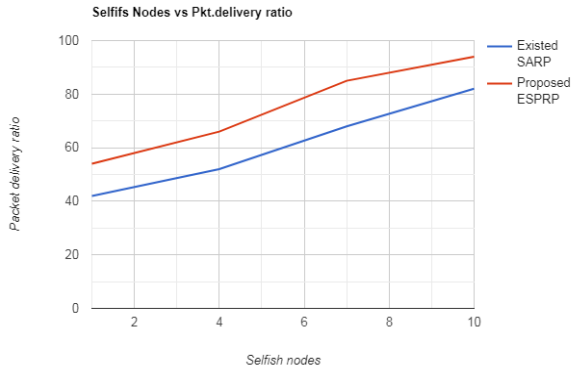

Fig. 8. Packet delivery ratio versus selfish nodes

Fig.8 demonstrates the ratio of packet delivery attained with the proposed protocol. The improved packet delivery ratio is achieved by choosing stable paths. The proposed protocol. As with other routing protocols, increasing numbers of nodes do not affect the delivery ratio for packets.

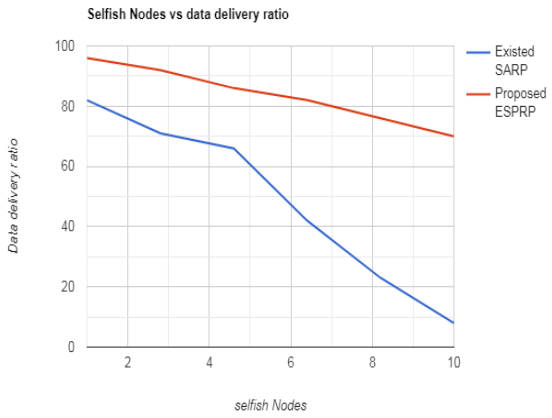

Fig. 9. Data delivery ratio versus selfish nodes

Fig. 9 indicates two techniques versus selfish nodes in the data delivery ratio. The delivery ratio decreases for the existing method with an increase in the number of selfish nodes. But even so, ESPRP can provide the best delivery ratio for node packets, the number of packets delivered is around 70 %.

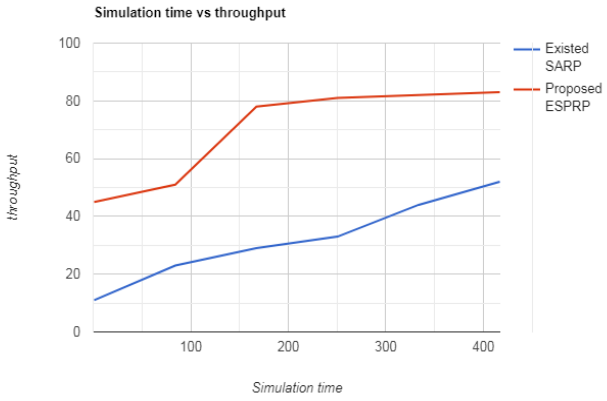

Fig.10. Throughput versus simulation time

In Figure 10, the level of performance shows a very high level of throughput, even if the simulation time provided is about 100%. The cross-layered protocol technique allows a high throughput as related to existed protocol.

V. CONCLUSION

Cognitive radio networks have no centralized security control, so nodes endure from different types of attacks. However one of the prevalent attacks is a selfish node attack by which a node attempts to offer its neighbours maximum possible services without ever offering its services. We used NS-2.35 C++-based discrete event simulator can efficiently simulate an independent node detection. Mostly from the results of the simulation, we can conclude that the work proposed shown the data delivery ratio and Packet delivery ratio is improved considerably. Computing overhead is reduced greatly, simultaneously traffic data flows through selfish nodes were penalized and the delivery ratio was lowered. The proposed system works well with several sessions for different sized networks. This proved to harm efficiency, reliability, and fairness in cognitive radio networks through the selfish node detection approach.

REFERENCES

1. Hossain, E.; Niyato, D.; Kim, D.I. Evolution and Future Trends of Research in Cognitive Radio: A Contemporary Survey. Wirel. Commun. Mob. Comput. 2015, 15, 1530–1564.
2. Ahmad, A.; Ahmad, S.; Rehmani, M.H.; Hassan, N.U. A Survey on Radio Resource Allocation in Cognitive Radio Sensor Networks. IEEE Commun. Surv. Tutor. 2015, 17, 888–917.
3. Ma, Y.; Zhou, L.; Liu, K. A Subcarrier-Pair based Resource Allocation Scheme Using Proportional Fairness for Cooperative OFDM-based Cognitive Radio Networks. Sensors 2013, 13, 10306–10332.
4. Huang, J.; Zeng, X.; Jian, X.; Tan, X.; Zhang, Q. Opportunistic Capacity-based Resource Allocation for Chunk-based Multi-carrier Cognitive Radio Sensor Networks. Sensors 2017, 17, 175.
5. Sufyan, Nadeem, Saqib, Nazar Abbass, Zia, Muhammad, "Detection of jamming attacks in 802.11b wireless networks", EURASIP Journal on Wireless Communications and Networking 2013.
6. I.Ngomane ; M. Velempini ; S. V. Dlamini, "The detection of the spectrum sensing data falsification attack in cognitive radio ad hoc networks", 2018 Conference on Information Communications Technology and Society (ICTAS), May 2018.
7. L. Senecal, "Understanding and preventing attacks at layer 2 of the OSI reference model", 4th Annual

Communication Networks and Services Research Conference (CNSR'06), June 2006.
8. Guillermo Mario Marro, “Attacks at the Data Link Layer”, CiteSeerX 2003.
9. Kiam Cheng How1, Maode Ma1, and Yang Qin, “A Cross-layer Selfishness Avoidance Routing Protocol for the Dynamic Cognitive Radio Networks”, IEEE International Workshop on Recent Advances in Cognitive Communications and Networking 2011, pp. 942-946.
10. Khyati Patel, Aslam Durvesh, “Research Paper on Detection of Multiple Selfish Attack Nodes Using RSA in Cognitive Radio”, IJARIIE, Vol-2 Issue-3 2016