Jamming Avoidance using RED approach and cognitive networks in MANETs

Ms. Iqbaldeep Kaur, Ms.Navneet Kaur, Ms. Nafiza Mann, Ms.Isha Vats
Associate Professor, Assistant Professor, Assistant Professor, Assistant Professor
Department of computer Science and Engineering, Chandigarh Engineering College, Landran, Punjab, India

Abstract - In wireless networks jamming attack is main problem and this can affect the network by various ways. Sometimes jammer retransmits messages to create jam over network or sometimes jammers are radio jammer which disturbs communication by decreasing the signal to noise ratio. Jamming can also be arise because of various different reasons like it can be intentionally created by attackers which lead to denial of service attack or it can be unintentionally created on network due to congestion. In previous researches various techniques are discussed to detect jamming. One way is to check the signal busy ratio. If channel is busy for long time that means there is a jam on network or it can be check by checking the threshold value. If threshold value exceeds up to some limit then there expect some jam on network. But there is still some work can be done. This attack can be prevented by blacklisting the nodes. It can be possible by applying check on nodes.

I. INTRODUCTION

A MANET is a kind of specially appointed system that can change areas and design itself on the fly. Since MANETS are portable, they utilize remote associations with join with different systems. This can be a standard Wi-Fi association, or an alternate medium, for example, a cell or satellite transmission [4]. A few MANETs are confined to a neighborhood remote gadgets, (for example, a gathering of PCs), others may be joined with the Internet. Case in point, A VANET (Vehicular Ad Hoc Network), is a kind of MANET that permits vehicles to speak with roadside gear [6]. While the vehicles might not have a direct Internet association, the remote roadside gear may be joined with the Internet, permitting information from the vehicles to be sent over the Internet. The vehicle information may be utilized to gauge movement conditions or stay informed regarding trucking armadas. As a result of the element way of MANETs, they are regularly not extremely secure, so it is critical to be careful what information is sent over a MANET.

II. COGNITIVE RADIO

A cognitive radio is a intelligent radio that can be modified and designed progressively[8][12]. Its handset is intended to utilize the best remote channels as a part of its region. Such a radio naturally distinguishes accessible directs in remote range, then in like manner changes its transmission or gathering parameters to permit more simultaneous remote correspondences in a given range band at one area [1]. This methodology is a type of element range administration. A CR "screens its own particular execution ceaselessly", notwithstanding "perusing the radio's yields"; it then uses this data to "focus the RF environment, channel conditions, join execution, and so forth.", and changes the "radio's settings to convey the obliged nature of administration subject to a proper mix of client necessities, operational restrictions, and administrative requirements"[9].

Types of cognitive radio:

- Full Cognitive Radio, in which each conceivable parameter detectable by a remote hub (or system) is considered.
- Spectrum-Sensing Cognitive Radio, in which just the radio-recurrence range is consider [2].

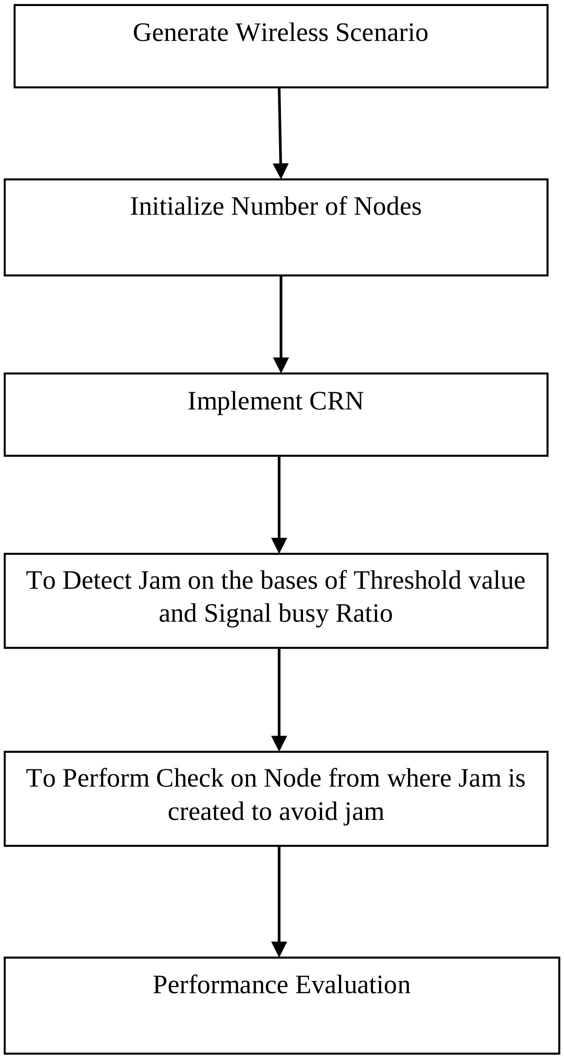
Different sorts are reliant on parts of the range accessible for cognitive radio:

- Licensed-Band Cognitive Radio, equipped for utilizing groups allocated to authorized clients (with the exception of unlicensed groups, for example, the U-NII band or the ISM band. The IEEE 802.22 working gathering is building up a standard for remote provincial zone system (WRAN), which will work on unused TV stations.
- Unlicensed-Band Cognitive Radio, which can just use unlicensed parts of the radio recurrence (RF) range [13]. One such framework is depicted in the IEEE 802.15 Task Group 2 determinations, which concentrate on the concurrence of IEEE 802.11 and Bluetooth.
- Spectrum versatility: Process by which a cognitive-radio client changes its recurrence of operation [5]. Cognitive-radio systems expect to utilize the range as a part of an element way by permitting radio terminals to work in the best accessible recurrence band, keeping up consistent correspondence prerequisites amid moves to better range.
- Spectrum offering: Spectrum imparting cognitive radio systems permits cognitive radio clients to impart the range groups of the authorized band clients. On the other hand, the cognitive radio clients need to confine their transmit control so that the obstruction brought on to the authorized band clients is kept underneath a certain edge[3][7].

III. PROBLEM FORMULATION

In wireless networks jamming attack is main problem and this can affect the network by various ways. Sometimes jammer retransmits messages to create jam over network or sometimes jammers are radio jammer which disturbs communication by decreasing the signal to noise ratio. Jamming can also be arise because of various different reasons like it can be intentionally created by attackers which lead to denial of service attack or it can be unintentionally created on network due to congestion. In previous researches various techniques are discussed to detect jamming. One way is to check the signal busy ratio. If channel is busy for long time that means there is a jam on network or it can be check by checking the threshold value. If threshold value exceeds up to some limit then there expect some jam on network. But there is still some work can be done. This attack can be prevented by blacklisting the nodes. It can be possible by applying check on nodes.

IV. FLOW OF WORK


Generate Wireless Scenario
Initialize Number of Nodes
Implement CRN
To Detect Jam on the bases of Threshold value and Signal busy Ratio
To Perform Check on Node from where Jam is created to avoid jam
Performance Evaluation

First of all we generate the wireless scenario. Then Initialize the number of nodes.After that implement the Cognitive Radio Network. Then detect the jam on the bases of Threshold value and Signal busy Ratio. After that perform the check on the number of nodes from where jam is created. In last we evaluate the parameters.

V. RESULTS

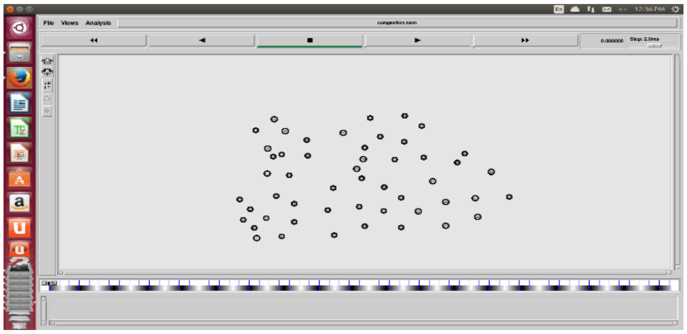


Fig 1. Initialization of nodes

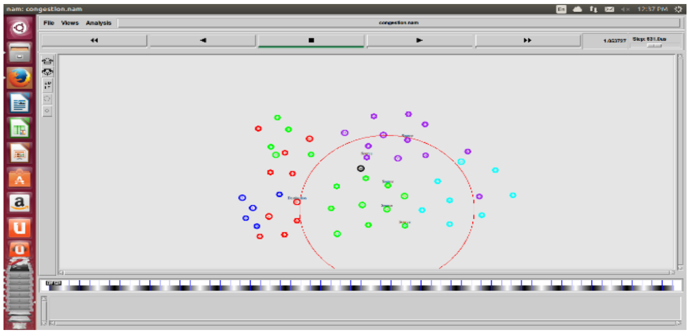
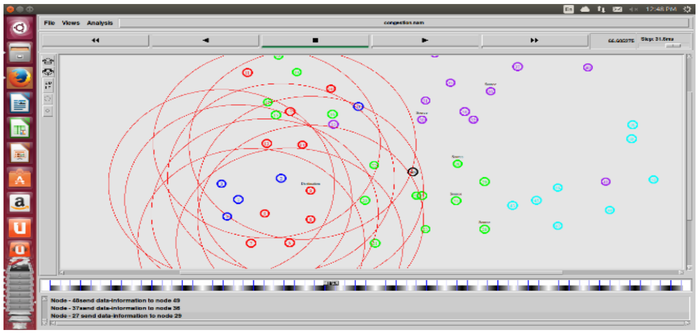


Fig 2. Initialization of Communication by Nodes



```
Node - 48send data-information to node 49
Node - 37send data-information to node 38
Node - 27 send data-information to node 29
```

Fig 3. Implementation of RED and Cognitive Network

LIFETIME OF NETWORK	
X-Time	Y-Energy
0	100
2	98
4	94
6	90
8	88
10	87

LOSS IN NETWORK	
X-Time	Y-Number of bytes
0	0
2	4
4	8
6	12
8	12
10	12

VI. CONCLUSION AND FUTURE SCOPE

In this paper, the threshold value for Random Early Detection has been examined in the Cognitive Network environment. The free channel utilization is used resulting effective control on jamming and further this work is analyzed on the parameters such as: Network Lifetime and Packet Loss. This work can be further enhanced with various number of parameters in different environments.

VII. REFERENCES

[1] Balogun, V, Krings, A. "An Empirical Measurement of Jamming Attacks in CSS Cognitive Radio Networks" Electrical and Computer Engineering (CCECE) 2014 IEEE 27th Canadian conference on IEEE, 2014.

[2] Amjad, M.F, Aslam, B, Zou, C.C. "DS3: A Dynamic and Smart Spectrum Sensing Technique for Cognitive Radio Networks Under Denial of Service Attack" Global Communications Conference (GLOBECOM), IEEE, 2013.

[3] Wenjing Wang. "Collaborative jamming and collaborative defense in cognitive radio networks" International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), IEEE, 2011.

[4] Marttinen, A., Wyglinski, A.M. , Jantti, R. "Statistics-based Jamming Detection Algorithm for Jamming Attacks Against Tactical MANETs" Military Communications Conference, 2014.

[5] Huahui Wang, Lightfoot, L., Tongtong Li "On PRY-layer Security of Cognitive Radio: Collaborative Sensing under Malicious Attacks" 44th Annual Conference on Information Sciences and Systems (CISS), 2010.

[6] Hyoungsuk Jeon, McLaughlin, S.W. , Il-Min Kim, Jeongseok Ha "Secure Communications with Untrusted Secondary Nodes in Cognitive Radio Networks" Wireless Communications, IEEE, 2014.

[7] Sorrells, C., Lijun Qian , Husheng Li "Quickest Detection of Denial-of-Service Attacks in Cognitive Wireless Networks" Conference on Homeland Security, 2012.

[8] Minho Jo, Longzhe Han, Dohoon Kim In, H.P. "Selfish attacks and detection in cognitive radio Ad-Hoc networks" Network, IEEE, 2013.

[9] Li, Xiaohua,Cadeau, W. "Anti-jamming performance of cognitive radio networks" 45th Annual Conference on Information Sciences and Systems (CISS), 2011.

[10] Martyna, J. "Power allocation games for cognitive radio networks with incomplete information" Networks & Digital Signal Processing (CSNDSP), 2012 8th International Symposium on Communication Systems, IEEE, 2012.

[11] Sharma, S., Singh, A.K. "On Detecting Termination in Cognitive Radio Networks" 17th Pacific Rim International Symposium on Dependable Computing (PRDC), 2011.

[12] Young-Hyun Oh,Thuente, D.J. "Channel Detecting Jamming Attacks against Jump-Stay Based Channel Hopping Rendezvous Algorithms for Cognitive Radio Networks" 22nd International Conference on Computer Communications and Networks (ICCCN), 2013.

[13] Sorrells, C., Potier, P., Lijun Qian, Xiangfang Li "Anomalous spectrum usage attack detection in cognitive radio wireless networks" International Conference on Technologies for Homeland Security (HST), 2011.

[14] Yulong Zou, Xuelong Li,Ying-Chang Liang "Secrecy Outage and Diversity Analysis of Cognitive Radio Systems" IEEE Journal on Selected Areas in Communications, 2014.

[15] Jia Min,Wang Xinyu, Guo Qing, Gu Xuemai "A multi-bit decision cooperative spectrum sensing algorithm in mobile scenarios based on trust valuations in cognitive radio context" International Symposium on Wireless Personal Multimedia Communications (WPMC), 2014.