INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Bee inspired secured protocol for routing in cognitive radio ad hoc networks

J Ramkumar[1]*, R Vadivel[2]

1 Assistant Professor, Department of Computer Science, VLB Janakiammal College of Arts and Science, Kovaipudur, Coimbatore, 641042, Tamil Nadu, India
2 Assistant Professor, Department of Information Technology, Bharathiar University, Coimbatore, 641046, Tamil Nadu, India

OPEN ACCESS

Received: 14-07-2020
Accepted: 30-07-2020
Published: 19-08-2020

Editor: Dr. Natarajan Gajendran

Citation: Ramkumar J, Vadivel R (2020) Bee inspired secured protocol for routing in cognitive radio ad hoc networks. Indian Journal of Science and Technology 13(30): 3059-3069. https://doi.org/10.17485/IJST/v13i30.1152

***Corresponding author**.

jramkumar1986@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Background: Enhancing security and minimizing the delay is a significant task present in all modern networks. Dynamic emerging problems like node failure, route failure, intrusions, and security attacks lead the network to failure. Hence, there exist needs for development of a protocol that detects the intrusions and find the better route to destination. **Objectives:** The main objectives of this research is to understand the issues and challenges in routing that rise dynamically in cognitive radio ad hoc network and propose a bio-inspired routing protocol to enhance security and routing efficiency which will result in reduced delay cum energy consumption. **Methods:** This study proposes Bee Inspired Secured Protocol (BISP) for routing in cognitive radio ad hoc networks that focuses on increasing the security before sending data packets and decreasing the overall delay. An instinctive characteristic of Bees towards searching for food is utilized to design the proposed routing protocol, which selects the better path to the destination. To enrich the security during data transmission, Rivest Shamir Adelman algorithm is applied. The proposed protocol analyzes the security level of the route and neighbor node energy level before sending the data. **Findings:** NS2.35 simulator used to evaluate the performance of BISP. Simulation results indicate that BISP has better performance than the existing protocol (i.e., WPIP and GRP) in terms of throughput, packet delivery ratio, reduced delay and enhanced security. **Novelty :** Comprehensive analysis indicates that BISP have superior performance in classifying the intruding nodes, enhancing the security of data getting transmitted, and reducing the delay.

Keywords: Routing; security; intrusion; Bee; CRAHN

1 Introduction

Cognitive Radio Ad Hoc Networks (CRAHN) are emerging as significant drivers in the ICT world. CRAHN users expect more enhanced data transfer rates, quality of experience and service to meet the diversification. To provide efficient and quality enabled services in CRAHN, wireless networks need to adopt new technologies

by importing a wide variety of functional networks. It includes Software Defined Network, Internet of Things, Cognitive Radio (CR) and End-to-End device technologies. The challenges in CRAHN get increased in parallel when technologies grow. In CRAHN, CR is identified as one of the promising technologies that gained the attention of industries and academia because it can solve the network issues fully or partially.

The performance of CRAHN in different communication scenarios is better when comparing with other wireless technology enabled networks. To meet the enhanced and growing complexity in CRAHN, it is necessary to improve autonomy and intelligence in it. In general, CR is a smart technology, i.e., CR has better efficiency in analyzing, sensing, and making decisions for allocating the dynamic resources and managing the spectrum. Few issues are still present in CR network's resource allocation like complexity, increased time for computation, a lengthier route to destination, route failure, and controlled optimization. To minimize emerging issues like this, CR users need to have a better ability to make decisions while interacting with different environments. Auspiciously, the artificial intelligence (AI) era is stepping-in. In the modern era of artificial intelligence, machines have awareness about creating interactions with varying environments like human beings. AI adopts optimization methodologies and clustering methodologies [(1)] to select the dynamic-channel and finding the best route. Optimization enables the smart allocation of dynamic resources to CR Primary-Users and CR Secondary-Users, where it takes optimum actions based on operating environments for enhancing the resource utilization of spectrum.

The nodes in CRAHN have minimum energy but deployed in the environment that has significant number of hazardous attacks [(2)], namely (1) forged injection of false information (2) misdirection of node (3) traffic and collision of the network (4) corrupting the memory. Nevertheless, much time was used and a massive volume of energy is required. The wireless network requires an undemanding and efficient method for rectifying the intrusions, which are made by both the insider-nodes and outsider-nodes.

Session Initiation Protocol (SIP) [(3)] proposed to solve various issues in the IP Multimedia Subsystem and minimize vulnerability to the phase of registration . Attacks called DDoS focused on the protocol system and structure further proposed for identifying the intrusion in a distributed system with its baseline techniques. Big Flow Approach [(4)] applied to progress a method of verification and validate the outcome of the classifier. Incremental change made to the classification model to carry out the experiments. The results portray the increased accuracy, which accompanied by a considerable amount of storage, lesser training time when compared with other models. Statistics based IDS [(5)] proposed to solve the problem of impurification for mixed signals at high dimension space. An innovative purification method-based analysis proposed and the maximum volume of the pure signals are obtained. Besides, a subspace mechanism for projection proposed as a part to detect and remove the outliers. Further, the efficiency of the algorithm was validated with the experimental result and it proved the better robustness against the noise. An IDS based on deep learning [(6)] was proposed with a feature mapping method, and a deep belief network with the multi-restricted vector machine. The SVM classifier applied for training and detecting the method. The results show its efficiency over other techniques. The application of a criterion-based method [(7)] proposed for selecting relevant features in IDS. Identification of 19 different techniques for data mining was made to analyze the strength and weaknesses of the detection system. A research gap and poor classification were detected. From the analysis, it was found that more extensive experiments in terms of real-time solutions could be provided.

An approach for detecting the intrusion to comprehend the potential of IoT [(8)] proposed in Edge-of-Things (EoT) based network. Based on the progression, a Belief Network implemented and various approaches were defined and structured where it was compared with the state-of-the-art techniques to prove its efficiency level of performance. Reliable IDS [(9)] proposed with the hybrid kernel for safeguarding the malicious network attack. Gravitational Search Algorithm with Differential Evolution also proposed for optimizing the parameters and Kernel Principal Component Analysis further introduced to reduce the dimension of the feature vector. An innovative intrusion detection approach was developed and applied to datasets called KDD99 and UNSW-NB15 to validate its accuracy and saving time benefit. Representation of an intelligent model [(10)] proposed to breach the security was performed with an enhanced Deep Learning algorithm called, Deep Belief Network. The malicious actions investigated for embedding the methodology of Deep Learning. The results analyzed with standard IDS to prove its efficiency. The application of the neural network model [(11)] proposed to detect the intrusion in the system. Fast optimization and better robustness were achieved and KDD CUP 99 dataset was used. Simulation results with a lesser false alarm rate and increased detection rate than other traditional algorithms show the effectiveness. A system model for the prediction of sequence-to-sequence [(12)] constructed for prediction of the sequence of system calls, where it aims to track the state of the system along with its prediction behavior. The experimental study validated with the test data and results shows that there was an increased performance over existing algorithms.

An IDS based on Feed Forward Deep Neural Networks [(13)] was an ensemble with a filtering-based feature selection method to detect the intrusion in modern networks. The evaluation made with the NSL-KDD dataset. Comparison with other algorithms namely, Naïve Bayes, decision tree and SVM made to prove its efficiency. A scheme for detection of intrusion detection [(14)] was

performed which was based on machine learning. The complexity of the client network was reduced wherein the screening of multi-layer traffic with virtual machine selection was performed. Experimental results proved to indicate its efficiency in detecting the intrusion. Designing of a novel intelligent based system[15] with implemented feature selection for the hybrid approach was proposed. The features computed based on the probability estimated. Rough Set (RS) theory utilized to segregate the data into upper and lower approximations. The quantitative data sets compared to reducing the complexity of training and false alarm rate. The classifiers of the proposed method compared with the existing techniques for better performance. IDS based clustering cum feature selection algorithm[16] implemented with wrapper and filtering methods called, Feature Grouping depending on Linear Correlation Coefficient methodology with Cuttlefish Algorithm (CFA). Classifier called Decision Tree used for classification and KDD Cup 99 dataset used for validating its performance. Hybrid Feature Selection with a two-level classifier[17] proposed with the integration of the two-level ensemble method and the NSL-KDD dataset utilized for the study. The result showed that it has increased performance, which works better than state-of-art methods. A statistical test was conducted to validate the classifier. Load Balancing Opportunistic Routing[18] and Bee Inspired Agent Based Routing[19] proposed to enhance the routing process in CRAHN by without considering the security issues.

Routing indicates the process of finding a path to the destination in a network (i.e., from source to destination). The processes[20] involved in routing are (i) sharing of routing information to neighbor nodes, (ii) managing the route failure, (iii) reforming the feasible path. For performing the sufficient operations in the network, ad-hoc routing protocols should meet the below-mentioned requirements:

- **Minimal time for discovering the route:** Time spent on determining the route for a specific destination should be low.
- **Minimum control overhead:** Packets used for discovering and maintaining the route should be minimized to save the bandwidth and avoid collisions.
- **Loop free route:** Selection of route having loop will end with unnecessary usage of bandwidth, undelivered data packets, and continuous movement of data packet in the network.
- **Reconfiguration of route:** Protocol should have the capability of reconfiguring the routes that have a high frequency of changes and disconnect.

Different protocols are being proposed to overcome the issues in CRAHN, but still CRAHN is facing many issues like high delay, energy consumption, critical routing and intrusions. So far, protocols proposed for ad-hoc networks like CRAHN focus only on one objective, (i.e., finding the best route) but did not consider security about the data. This research work has aimed to develop a protocol that can effectively perform different actions like (i) detecting the intrusion (ii) finding the ideal route to destination (iii) providing better security to data (iv) minimize the delay and energy consumption.

2 Proposed methodology

The CRAHN has huge roles in new fields and the network needs an adequate routing procedure for efficient data transmission between nodes. More applications attracted the CRAHN environment, and CRAHN's security level needs to be effective. Yet new developments in CRAHN security offer the network some protection. It demands a few additional controlling methodologies to enhance the security of the network internally and externally. Yet delivering network protection is a big challenge, as it will secure any bit of information from attackers. The transmission of data from the source-node to destination-node through neighbor nodes is generic; however, the choice of secured communication path should avoid attacker interference. The routing protocol proposed in this protocol is bee colony focused. The various stages involved in the proposed routing protocol are:

- Selecting the nearest nodes
- Path uncovering
- Path selection
- Providing security to the path
- Forwarding of data

The scout bee role in this protocol is to find the shortest cum best path; also, it can be indicated as a path to the food source, from source to destination. In real-time, bees releases an odor, treated as a signal that assists in identifying the source of food and marks the exact path to the source of the food. The shortest route usually has a high fragrance (i.e., the odor) signal response as compared with other routes. It is possible to divide the scout bees into the primary scout bee (PSB) and the secondary scout bee (SSB). Those two kinds of bees are used for requesting a path and reply to the request.

2.1 Selecting the nearest nodes

The operation of selecting the nearest node is performed once the network route is chosen, i.e., by ending the whispering signals (i.e., *HELLO* messages) to the adjacent nodes. A separate table is utilized for the management of routing information, node statistics, node identity, route Identity, source and destination identification, node length, energy level, trust value, etc. The data is also gathered from answers received by the nearest nodes.

2.2 Path uncovering

In the path uncovering stage, the source node transmits the different numbers of primary Scout bees (i.e., PREQ packets) to the nearest random nodes during this path uncovering phase. The primary task of PSB is to transmit the data via the nearest nodes and assist the food source classification. The destination node gets multiple requests from the different nodes randomly and it gives an obstacle for several scout bees in reaching the scot bees. The reason falls as a time limit, the collision between nodes, failure of the path, and other routing-related assaults. Target nodes attempt to send Path Reply (i.e., PREP) messages with the assistance of SSB. The security of the paths is taken care of by these bees. The mechanism of path protection is introduced and it is indicated as false (or 0) to denote the path is not secured. Indication of the path as true (or 1) signifies the secured path and there exists no need for the incorporation of security algorithm. An essential aspect of path discovering is to generate the predetermined PSB and the value of trust level is used for that. Such values are determined for the nodes before the data arrives without any difficulties in the destination. The SSB also uses it to check whether the return path is correct. Description of the key Scout bees and the confidence worthiness are provided for the destination node. The secondary node to pass the data to the sink node utilizes trust values. If the path is inconsistent, the security mechanism for secure communication between the nodes will be initiated.

2.3 Path selection

Path selection is made by collecting detailed information about the trust value, level of energy available and time, etc. from the SSB. It also offers the details of the detection of route assaults. Once that information is collected for route selection, a sink node receives different SSB PREP packets. Consider SB1, SB2, SB3, SB4 and SB5 as scout bees that roam via the different number of nodes for reaching the destination node (i.e., the food source), and P1, P2, P3, P4 and P5 as the paths for SB in reaching the destination node. If a scout bee starts its progression towards the destination node from the sink node, then it will not receive any better idea about the destination. Following two scenarios are considered for path selection:

Scenario 1 If, for example, Sb2 hits the goal node easily through Ph2, we do not see any barriers or difficulties along this particular direction so that it can be treated as a clear route to the aim node. This specific path has a high degree of fragrance that lets the scout bee track the source of food (destination node). For further usage, the confidence factor of the route and the node is determined. If SB3 reaches the destination node by making use of P4, then it immediately creates a comparison with other paths. This scenario makes a consideration that there exist no issues (or obstacles) in the selected path and it is treated as a safe path in reaching the destination node. Alternatively, it can be said as the chosen path has increased concentration of odor and assists SB to identify the source of food (i.e., destination node). Computation of Trust level for each node and path is necessary for further use. Eq.(1) is used for calculating the trust level.

$$Rank_{sel} = \frac{1}{M}\left(w + (g-w)\frac{i-1}{N-1}\right)\ i \in \{1,2,3,\ldots N\} \tag{1}$$

where N indicates the Rank, w represents the Worst SSB node; g denotes the Best SSB node.

To make communication in a secured manner, it is necessary to calculate the trust level of a secured path and data. The calculation of overall trust is also essential. If the level of trust is received as 1 then it indicates no need for the usage of security, but if it is 0 then it shows the usage of security. A comparison of trust level values is made in Many-to-Many manner with other paths and scout bees. At last, SSB gathers and brings the collected information to sink node from the destination node

$$Initial_{TLR} = \frac{Positive_{FB} + Negative_{FB}}{Total_{FB} + Positive_{FB}} \tag{2}$$

$$Level\_of\_Security_p = \frac{Estimated\_Security_p}{Actual\_Security_p} \times (FB)\ ,\ \ p = 1,2,\ldots n \tag{3}$$

$$Overall\_Trust = \sum Initial_{TLR} + Level\_of\_Security_p \tag{4}$$

$$Trust\_data = \sum Overall\_Trust - Data_{FB} + Energy\_Consumed_{FB} \tag{5}$$

Scenario 2

In this scenario, it is assumed that two SSB identifies a unique path to the source of food having equal hop count, distance, and lifespan. Every SSB tries to achieve the sink node cum other node support towards deciding to select the better path. This research work makes use of a method, namely "Rank Selection Process (RSP)" for evaluating individual paths. When SSB enters the destination node, a ranking process is initiated. Once the secondary scout bee enters the destination node, the process of rank selection is initiated. The values for the fitness can be allocated as energy level or confidence of the path. Distribution of ranks is done according to their fitness values through the collection of secondary scout bees.

RSP concedes categorization of chosen SSB involves the below steps:

1. Based on the trust level value (i.e., the fitness value), SB is ordered in a decreasing manner.
2. Assign a rank value for SSB based on its trust level value.
3. Assess the energy level and trust level value of every SSB.

2.4 Providing security to the path

Only when the trust level value is zero, then the security phase is executed, else no. This research work makes use of handshake methodology to proceed the security phase, and it involves the below stages:

1. Whispering messages (i.e., Hello Message) are sent to the neighbor node by SSB.
2. Once after receiving the whispering message, the neighbor node sends an acknowledgment and sends its whispering message to the SSB.
3. Once after receiving the acknowledgment message, SSB sends its data to the neighbor node. In Parallel, it accepts the whispering message of its neighbor.
4. Once after receiving the SSB data, the neighbor node sends acknowledgment as the confirmation of receiving the data.
5. If there arises a necessity of providing security, then RSA security is applied for avoiding the malicious node intrusion in CRAHN.

This research work utilizes the Rivest Shamir Adelman Algorithm [21] for providing security for the data that is sent across the CRAHN.

1. Choose two huge prime number A and B
2. Compute $N = A \times B$
3. SSB computes the public key E (i.e., used for encryption), with the condition of having (A-1) and (B-1) as not a factor.
4. Neighbour computes the private key D (i.e., used for decryption), which satisfies the below equation

$$(D \times E)\, mod\, (A-1) \times (B-1) = 1 \tag{6}$$

5. To encrypt, compute CT (i.e., ciphertext) from PT (i.e., plain text) by using the below equation

$$CT = PT^E modN \tag{7}$$

6. SSB transmits CT as an encrypted text to the neighbor node.
7. To decrypt the CT, neighbor node computes PT from CT using the below equation

$$PT = CT^D modN \tag{8}$$

2.5 Forwarding of data

SSB applies the procedure mentioned in the above step is used to provide security. Once after completing the security phase, SSB reaches the sink node to pass the information that the current path is secured and better for making the communication.

3 Simulation setting

The current section makes a discussion about evaluating the BISP using NS2 simulations. In general, there exists no trusted simulator for evaluating protocols for CRAHN. Furthermore, the details that are available regarding the protocol implementation or simulation for CRAHN are unclear to understand, especially the performance of protocols. This paper attempts to compare BISP against WPIP[22] and GRP[23]. This research work prefers the C++ language to use in the NS2 simulator. Table 1 shows the simulation setting used for evaluating the proposed protocol.

Table 1. Simulation Settings and parameters

Parameters of Simulation	Values
Simulation Area Size	$2500 \times 2500\ m^2$
Simulator Name and Version	*NS*2.35
Count of nodes	10 *to* 100 *varying with* 10
Mobility Model	*Randomway Point*
Speed of Mobility	$4\ m/s$ *to* $40\ m/s$
Type of Traffic	*Constant Bit Rate*
Type of Channel	*Wireless*
MAC	802.16
Transmission Range	$500\ m$
Initial Energy	15 *Joules*
Size of Packet	$0.512\ kb$

4 Performance metrics

This research works makes use of below mentioned metric for analyzing the performance of proposed protocol BISP against WPIP[22] and GRP[23].

- **Throughput:** Measure of the overall quantity of data transmitted (or processed) from source to destination in a threshold time
- **Packet Delivery Ratio:** Measure of packets successfully received in destination against total packets sent by the source
- **Packet Drop:** Percentage of packets that not yet reached the destination due to different reasons like route failure, node failure, expiry of the packet, etc
- **Delay:** Consumed time by the protocol to deliver the packet to the destination
- **Energy Consumption:** Energy consumed to deliver the packet to the destination from the source.

5 Results and Discussion

5.1. Throughput analysis

Figure 1 presents the throughput of routing protocols against node count. It is clear to understand that when the number of nodes gets increased, then throughput for all protocols too increases. The reason for this is when there is an increase in node count, and then it leads to enhancement in the count of broadcasted messages in route discovering process which in turn enhances the throughput. The results indicate that the throughput of WPIP and GRP is averagely 15.25% lower than BISP, and this is due to, BISP taking energy and distance metric into consideration that decreases flooding of broadcasting packets. Corresponding values of Figure 1 is shown Table 2.

Table 2. Throughput Vs Nodes

Node Count Protocols	10	20	30	40	50	60	70	80	90	100
BISP	75	73	71	68	65	63	61	59	57	55
WPIP	71	69	64	63	61	59	57	55	52	50
GRP	59	57	53	52	50	47	46	44	42	41

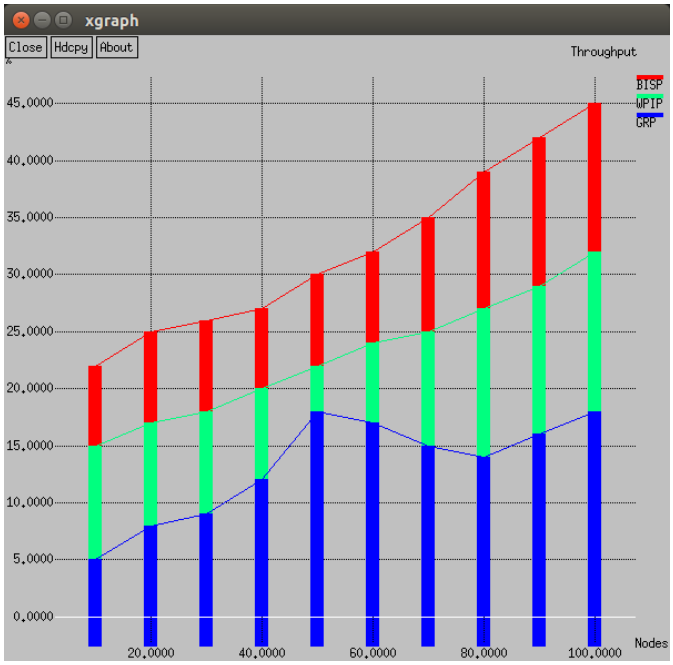

Fig 1. Throughput analysis

5.2 Packet delivery ratio analysis

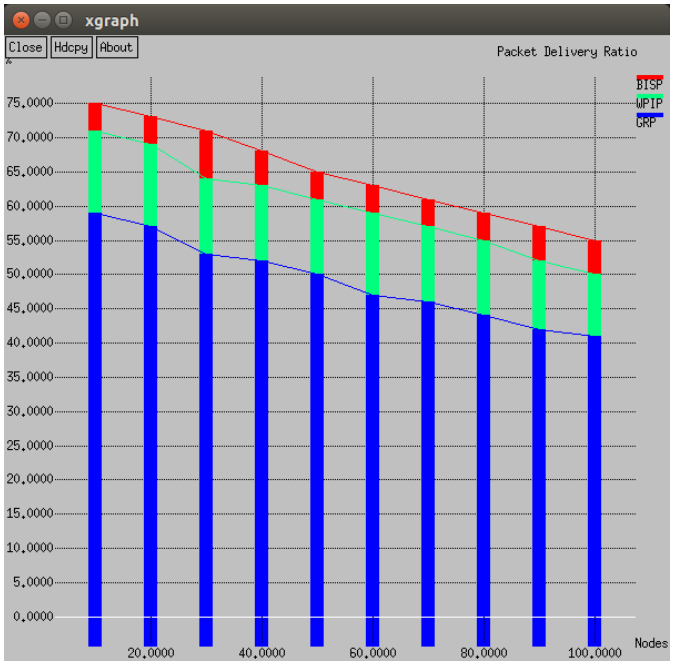

Fig 2. Packet delivery ratio

Figure 2 presents the packet delivery ratio against node count. It is conspicuous that the packet delivery ratio gets decreased when the count of nodes gets increased for all the protocols. This is because an increase in node count leads to the situation of unsecured network cum multiple breaks in route, and hence there exists a degrade in delivering the packets to the destination.

The results demonstrate that the packet delivery ratio of WPIP and GRP is averagely 10.1% minimum that BISP. The main reason for this is, BISP intakes the distance metric when choosing the neighbor node that assures a stable path between two nodes that makes communication while it moves in maximum speed. Corresponding values of Figure 2 is shown Table 3.

Table 3. Packet Delivery Ratio Vs Nodes

Node count Protocols	10	20	30	40	50	60	70	80	90	100
BISP	75	73	71	68	65	63	61	59	57	55
WPIP	71	69	64	63	61	59	57	55	52	50
GRP	59	57	53	52	50	47	46	44	42	41

5.3 Packet drop ratio analysis

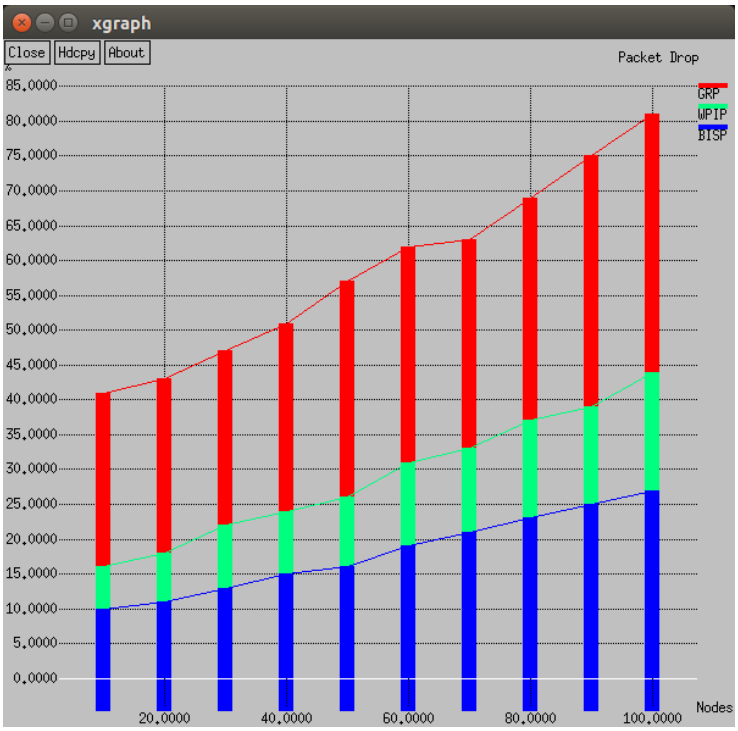

Fig 3. Packet drop analysis

Analysis of the overall packet drop against the node count is shown in Figure 3 . It was evident that the drop rate of packet increases when node count increases because there exists a more chance for (i) presence of malicious nodes and (ii) some node start acting greedy to save energy. The main reason for the increase in packet drop is, the network starts losing its stability when the nodes get increased. The results evident that BISP has a lower packet drop than the other two protocols. BISP has a 25.95% lower packet drop than the other two protocols. This is because the route discovering process works well in BISP. Corresponding values of Figure 3 is shown Table 4 .

5.4 Delay analysis

Delay analysis of proposed protocol against the existing protocols presented in Figure 4. It indicates that an increase in node count will increase the delay. Making utilization of security mechanism enhances the delay more. When analyzing the protocols for the delay, it was found that BISP is also facing delay when node count increases, but after a certain level, the delay gets reduced. While analyzing WPIP and GRP protocols, it is clear to understand that the presence of delay keeps on get increased

Table 4. Packet Drop Vs Nodes

Node count Protocols	10	20	30	40	50	60	70	80	90	100
BISP	10	11	13	15	16	19	21	23	25	27
WPIP	16	18	22	24	26	31	33	37	39	44
GRP	41	43	47	51	57	62	63	69	75	81

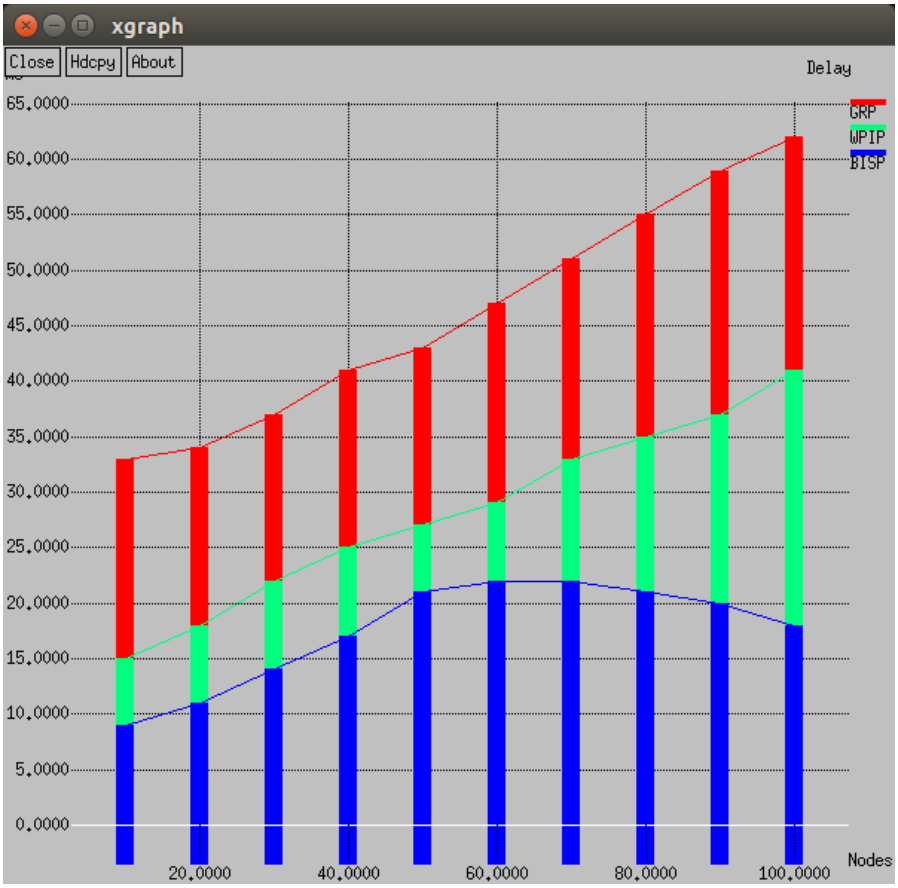

Fig 4. Delay analysis

when node count increases. The main reason for that is WPIP and GRP chooses the node that low energy for forwarding the packet that results in route failure. Corresponding values of Figure 4 is shown Table 5.

Table 5. Delay Vs Nodes

Node count Protocols	10	20	30	40	50	60	70	80	90	100
BISP	9	11	14	17	21	22	22	21	20	18
WPIP	15	18	22	25	27	29	33	35	37	41
GRP	33	34	37	41	43	47	51	55	59	62

5.5. Energy consumption analysis

The overall energy consumption versus node count demonstrated in Figure 5. It is indisputable that the energy consumption of BISP is considerably lower when comparing with WPIP and GRP. High consumption of energy indicates the instability of

the protocol when node count is increased. BISP has consumed the acceptable range of energy only (i.e., 17.4%), but WPIP has consumed 34.6%, and GRP has consumed 46.8%. This is because during the route discovering process nodes that are located in the range 0.4R<d<0.6R will alone get a presence in the route formation, that is to the destination node. In short, nodes that are located very close to the sending node won't participate in the route discovering cum route formation process. Corresponding values of Figure 5 is shown Table 6 .

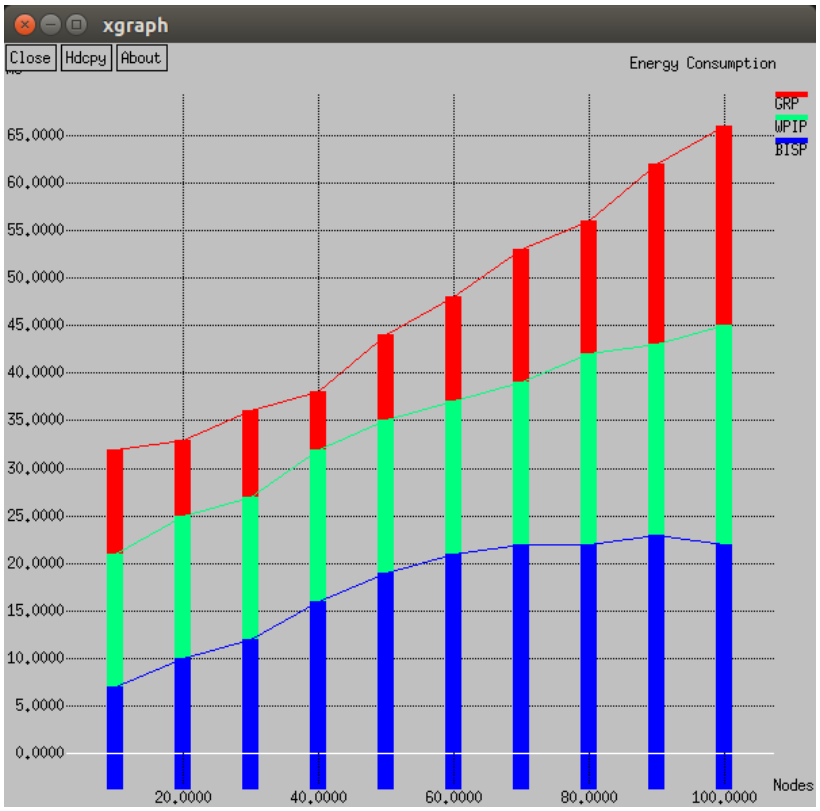

Fig 5. Energy consumption analysis

Table 6. Energy Consumption Vs Nodes

Node count Protocols	10	20	30	40	50	60	70	80	90	100
BISP	7	10	12	16	19	21	22	22	23	22
WPIP	21	25	27	32	35	37	39	42	43	45
GRP	32	33	36	38	44	48	53	56	62	66

6 Conclusion

This study has proposed a BISP security mechanism based on the instinctive characters of bees. The BISP has an influence on dealing with malicious nodes inside the network and secures the data packet before the transmission. Nevertheless, the utilization of instinctive characters of bee towards the detection of malicious nodes has confined improvement. The routing concept can be an ensemble with a trusted cryptographic algorithm to ensure the security of data getting transmitted to the destination. The proposed protocol performance has been evaluated using selected performance metrics in the network simulator. The simulation study shows that the proposed protocol has improvement in performance based on energy consumption and delay compare with WPIP and GRP protocols. The results of BISP advance WPIP and GRP in terms of enhanced throughput and packet delivery ratio, reduced delay, packet drop and energy consumption. Follow-up work will examine the malicious and intruding nodes by applying the machine learning algorithms with different parameter.

References

1) Jihong W, Wenxiao S. Survey on cluster-based routing protocols for cognitive radio sensor networks. *Journal on Communications*. 2018;39:156–169. Available from: https://doi.org/10.11959/j.issn.1000-436x.2018244.
2) El-Malek AHA, Aboulhassan MA, Abdou MA. Evolutionary computation technique enhancing the performance of cognitive radio networks with energy harvesting. *Ad Hoc Networks*. 2020;107:102254–102254. Available from: https://dx.doi.org/10.1016/j.adhoc.2020.102254.
3) Manan J, Ahmed A, Ullah I, Merghem-Boulahia L, Gaïti D. Distributed intrusion detection scheme for next generation networks. *Journal of Network and Computer Applications*. 2019;147:102422–102422. Available from: https://dx.doi.org/10.1016/j.jnca.2019.102422.
4) Viegas E, Santin A, Bessani A, Neves N. BigFlow: Real-time and reliable anomaly-based intrusion detection for high-speed networks. *Future Generation Computer Systems*. 2019;93:473–485. Available from: https://dx.doi.org/10.1016/j.future.2018.09.051.
5) Zhang Y, Zhao L, Qu H, Han Z. Purification of mixed optical fiber intrusion signal by simplex volume analysis. *Optik*. 2019;194:163096–163096. Available from: https://dx.doi.org/10.1016/j.ijleo.2019.163096.
6) Yang H, Qin G, Ye L. Combined Wireless Network Intrusion Detection Model Based on Deep Learning. *IEEE Access*. 2019;7:82624–82632. Available from: https://dx.doi.org/10.1109/access.2019.2923814.
7) Salo F, Injadat M, Nassif AB, Shami A, Essex A. Data Mining Techniques in Intrusion Detection Systems: A Systematic Literature Review. *IEEE Access*. 2018;6:56046–56058. Available from: https://dx.doi.org/10.1109/access.2018.2872784.
8) Almogren AS. Intrusion detection in Edge-of-Things computing. *Journal of Parallel and Distributed Computing*. 2020;137:259–265. Available from: https://dx.doi.org/10.1016/j.jpdc.2019.12.008.
9) Lv L, Wang W, Zhang Z, Liu X. A novel intrusion detection system based on an optimal hybrid kernel extreme learning machine. *Knowledge-Based Systems*. 2020;195:105648–105648. Available from: https://dx.doi.org/10.1016/j.knosys.2020.105648.
10) Balakrishnan AN, Rajendran A, Pelusi D, Ponnusamy V. Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things. *Internet of Things*. 2019. Article ID 100112. Available from: https://doi.org/10.1016/j.iot.2019.100112.
11) Yang A, Zhuansun Y, Liu C, Li J, Zhang C. Zhang Design of Intrusion Detection System for Internet of Things Based on Improved BP Neural Network. *IEEE Access*. 2019;7:106043–106052. Available from: https://doi.org/10.1109/ACCESS.2019.2929919.
12) Lv S, Wang J, Yang Y, Liu J. Intrusion Prediction With System-Call Sequence-to-Sequence Model. *IEEE Access*. 2018;6:71413–71421. Available from: https://doi.org/10.1109/ACCESS.2018.2881561.
13) Kasongo SM, Sun Y. A Deep Learning Method With Filter Based Feature Engineering for Wireless Intrusion Detection System. *IEEE Access*. 2019;7:38597–38607. Available from: https://dx.doi.org/10.1109/access.2019.2905633.
14) Dey S, Ye Q, Sampalli S. A machine learning based intrusion detection scheme for data fusion in mobile clouds involving heterogeneous client networks. *Information Fusion*. 2019;49:205–215. Available from: https://dx.doi.org/10.1016/j.inffus.2019.01.002.
15) Prasad M, Tripathi S, Dahal K. An efficient feature selection based Bayesian and Rough set approach for intrusion detection. *Applied Soft Computing*. 2020;87:105980–105980. Available from: https://dx.doi.org/10.1016/j.asoc.2019.105980.
16) Mohammadi S, Mirvaziri H, Ghazizadeh-Ahsaee M, Karimipour H. Cyber intrusion detection by combined feature selection algorithm. *Journal of Information Security and Applications*. 2019;44:80–88. Available from: https://dx.doi.org/10.1016/j.jisa.2018.11.007.
17) Tama BA, Comuzzi M, Rhee KH. TSE-IDS: A Two-Stage Classifier Ensemble for Intelligent Anomaly-Based Intrusion Detection System. *IEEE Access*. 2019;7:94497–94507. Available from: https://dx.doi.org/10.1109/access.2019.2928048.
18) Duan W, Tang X, Zhou J, Wang J, Zhou G. Load Balancing Opportunistic Routing for Cognitive Radio Ad Hoc Networks. *Wireless Communications and Mobile Computing*. 2018;2018:1–16. Available from: https://dx.doi.org/10.1155/2018/9412782.
19) Palanisamy R, V M. BEE INSPIRED AGENT BASED ROUTING PROTOCOL-SECONDARY USER (BIABRP-SU). *International Journal of Engineering and Technology*. 2017;9(1):85–92. Available from: https://dx.doi.org/10.21817/ijet/2017/v9i1/170901407.
20) Srivastava A, Gupta MS, Kaur G. Energy efficient transmission trends towards future green cognitive radio networks (5G): Progress, taxonomy and open challenges. *Journal of Network and Computer Applications*. 2020;168:102760–102760. Available from: https://dx.doi.org/10.1016/j.jnca.2020.102760.
21) Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. 1978;21(2):120–126. Available from: https://dx.doi.org/10.1145/359340.359342.
22) Ramkumar J, Vadivel R. Performance modeling of bio-inspired routing protocols in Cognitive Radio Ad Hoc Network to reduce end-to-end delay". *International Journal of Intelligent Engineering and Systems*. 2019;12:221–231. Available from: https://doi.org/10.22266/IJIES2019.0228.22.
23) Jin X, Zhang R, Sun J, Zhang Y. TIGHT: A geographic routing protocol for cognitive radio mobile Ad Hoc networks. *IEEE Transactions on Wireless Communications*. 2014;13:4670–4681. Available from: https://doi.org/10.1109/TWC.2014.2320950.