An Intrusion Detection System for MANET based on Cuckoo Search Algorithm and Decision Tree

N. Kaur[1*], K.Sharma[2]

[1,2] Department of Computer Science and Engineering, Guru Nanak Dev Engineering College, Ludhiana, India

[*]*Corresponding Author: navpreetj15@gmail.com, Tel.: 8968559944*

Abstract— With increasing use of wireless networks there is increase in the number of intruder in networks. This could be explained by taking the example of the Mobile ad-hoc Network, as it is a network with no fixed infrastructure, security is the main issue in this network. During the transmission of data from source to destination, any node in network can act as an intruder .The intruder will not allow the successful transmission of the data. So, Intrusion detection system using cuckoo search and decision tree has been designed to detect the intruder node and exclude it from the network. The outcome has been depicted using MATLAB simulator using 45 to 60 nodes. For these nodes there are number rounds for which nodes are plotted. From each round the affected nodes are calculated on the basis of energy consumed by the nodes. The node which consumes maximum energy is the intruder in the network. Optimization of various QOS parameters is performed using Cuckoo search algorithm. The detected intruder is presented using decision tree.

Keywords— MANET,Cuckoo search algorithm, Intrusion Detection system,Decision Tree.

I.   INTRODUCTION

MANET stands for Mobile Ad-hoc Network .It is a continuously self-arranging infrastructure less network of various mobile devices connected wirelessly. The absence of a system framework gives extraordinary difficulties in these systems. All nodes are associated by means of remote connections. As network topology changes, MANET nodes can move openly in any direction. It can change its links to other devices as frequently. The hubs are arbitrarily associated with one another utilizing self-assertive topology. They can act as both routers and hosts. The main challenge in building a MANET is the supply of each device to keep the information needed to properly route the traffic. More frequent tearing connections and re-associations put an energy constraint on mobile nodes. As MANETs are illustrated by limited bandwidth and mobility nodes, there is a demand considering the energy efficiency of the nodes[1]. The routing protocols specially designed for wireless systems are used. In our research work , AODV protocol (Ad-Hoc On Demand Distance Vector)is used to establish a route from source to destination[2]. This protocol supports both unicast and multicast routing. This is an insecure advanced world. Security and antivirus programming are critical to any system. Intrusions can quickly become dangerous because hubs in specific systems can guarantee many roles. To remove intrusion from network intrusion detection system are designed in collaborations with various

optimization techniques. Intrusion detection system is a programming application or tool that scans system or framework for malevolent exercises. Malicious activities or intrusions are reported either to the administrator or to the security information and event management. Along with this there is a intrusion prevention system which has ability to respond to the detected intrusions. Intrusion detection system in our research work is designed with the collaboration to cuckoo search algorithm and decision tree[3]. Cuckoo search is the optimization technique used to optimize various Quality of Services parameters. CS is meta-heuristic in nature. It is more general and can be adjusted to a rationalization of the broader categories [4]. It is given by Yang and Deb is a nature enlivened calculation which depends on their forceful proliferation procedure that is few types of cuckoo lay eggs in another flying creature's home in a parasitic way. Decision Tree algorithm falls under the classification of the managed learning. They can be used to solve both regression and classification problems. It is the structure that includes root node, branches and leaf nodes. Each internal node represents a test on an attribute, each branch node represents outcome of the test and each leaf node represents class label. The top most node in the tree is the Root node. Decision tree learning uses a decision tree as a predictive model which maps observations about an item to conclusions about the item's target value. It is one of the predictive modelling approaches used in statistics, data mining and machine learning [5].

Rest of the paper is organized as follows, Section II contains the introduction to Mobile Ad-hoc Network, Section III describes the Intrusion Detection System in detail, Section IV explains briefly Cuckoo Search Algorithm, Section V consist of brief introduction to Decision Tree, Section VI contains the related work of Intrusion Detection System and Decision Tree, Section VII explains the methodology of proposed work with flow chart, Section VIII describes results and discussions of proposed work, and Section IX concludes the entire work along with the future scope.

II.   MOBILE AD-HOC NETWORK

 MANET stands for Mobile Ad-hoc Network. It is a continuously self-arranging infrastructure less network of various mobile devices connected wirelessly. MANET has multi-hop communication path with a radio link interconnected mobile nodes. MANET node via a mobile platform called composition can move freely in any direction at any speed and arrange them randomly. The nodes are limited in power, bandwidth and computing capacity. MANET has lack of central management and organization in advance, therefore, different from those of conventional network security problems exist. MANET wireless links make it easier to attack. Hackers steal and easier access to confidential information. They can also easily enter or leave a wireless network, because there is no physical connection. They can also directly network attacks to delete messages, or imitate a fake node in the bag injection. It violates the accessibility, reliability, authentication and non-repudiation of the destination network. User can also launch attacks damaged node from the network. A mobile ad hoc networks (MANET) for aerospace and military aviation, has highlighted the security issues. There are several existing measures that are trying to build a safe routing protocol for Ad hoc network and for providing protection for the attacks. The proposed solution is completely new with independent agreements, or in some cases, it incorporated into existing security protocols (such as DSR and AODV). The aim of these solutions focus on providing answers to specific attacks or attack set.

III.   INTRUSION DETECTION SYSTEM

Intrusion detection system is a programming application or tool that scans system or framework for malevolent exercises. IDS is also known as a packet sniffer which blocks data packets that travel along different reporting mediums. All the packets are examined after they are detected. The main motive of IDS is not only they prevent intrusion but also inform the administrators instantly when the intruder is attacking. IDS having sensors to identify signatures, some propelled IDS having a conduct activity to detect hostile response. Regardless of whether the signature doesn't coordinate with IDS, it can still tell about nature of attack. If

the signature coordinate, it will move to next stage or the link cut down from source IP, the data packet is dropped and a caution notifies the executive. If the signatures matches, the sensors pass the anomaly detection to check whether the packet that is received matches or not. If the packet has passed the anomaly stage, a stateful protocol analysis will be carried out. After this, with help of switch, the packets are put onto the network. If anything does not coordinates again, the connections are broken from the source IP address and the packet is destroyed, and ringing of the alarm notifies the administrator about the attack.

IV.   CUCKOO SEARCH ALGORITHM

Cuckoo Search (CS) is another heuristic meta-heuristic nature, in any application in almost no printing. In addition, and other existing meta-heuristic calculations (PSO, GA) associated method is unique. Cuckoo Search is a populace for calculation as like Genetic Algorithm and Particle Swarm Optimization, however, the determination instrument is distinctive and it is more like congruity inquiry. The randomization is more effective as the progression length is overwhelming followed and hence any huge stride is conceivable. CS fulfills two essential attributes of present-day meta-heuristic calculation:
* Increase and,
* Expansion

Increase alludes to the way that the issue at first hunt down ebb and flow the best arrangement and after that at last hunts down worldwide arrangement. Expansion implies the calculation that investigates the inquiry space proficiently. It gives a vast change by a limitless mean. The means shape an arbitrary walk prepare by a power-law step-length circulation by a substantial tail. A portion of the novel arrangements is created by Levy walk adjacent to the best arrangement acquired as such, this velocity to the neighbourhood look. Nonetheless, some portion of the new arrangements is created by mulling over the randomization idea. In any case, whose areas ought to thoughtfully be sufficiently far from the present best arrangement, this guarantees the framework does not get caught in a nearby ideal.

V.   DECISION TREE

Decision Tree algorithm falls under the classification of the managed learning. They can be used to solve both regression and classification problems. It is the structure that includes root node, branches and leaf nodes. Each internal node represents a test on an attribute, each branch node represents outcome of the test and each leaf node represents class label. Decision tree constructs classification or regression models in the form of a tree structure. It splits a dataset into smaller subsets while at the same time an related decision tree is developed step by step. The final tree consist of decision nodes and leaf nodes. A decision node has more than two

branches . Leaf node represents a classification or decision. The topmost decision node in a tree which is the best predictor is called root node. Decision trees can handle both explicit and analytical data. Decision tree approaches are used because of their simplicity. Figure 1 shows the basic splitting of the decision tree. Firstly the root node is divided into two decision nodes. Then the decision node on left side is divided into the terminal node and decision node. The decision node which is on the right side is divided into two terminal nodes which in all represents a Branch or Sub-tree. Splitting is continued till all leaf nodes are terminal nodes.
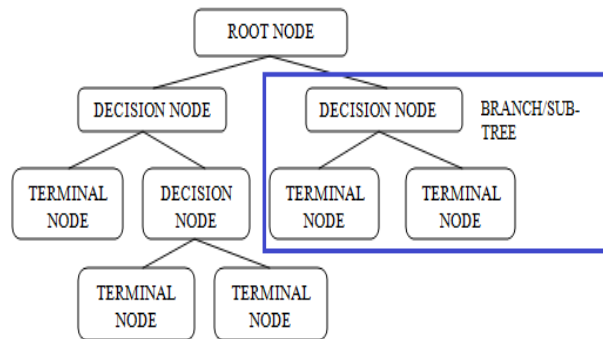

Figure 1. Decision Tree

VI.   RELATED WORK

Alex Hinds, *et al.*[6], focused on the range of available MANET routing protocols and discussed several features ranging from early protocols (e.g. DSDV) to higher level (e.g. MAODV).Protocol focused on Perkins' efforts to develop and improve routing of MANET. The series of research is related to the MANET routing domain has been found out and analyzed, and the state of art approaches identifies trends in research papers, like an exclusive use of a stochastic waypoint movement system, not including key parameters from results, rather than contrasting protocol performance to accessible alternatives.

Yuan, *et al.*[7], proposed that in the present age of the Internet, arrange traffic expanded exponentially, either dependent on client interest for system assets, QoS booking, or as per the advancement pattern of system applications for extension change of the current system, different applications in system traffic should be grouped and distinguished precisely, organize traffic characterization is especially significant. C4.5 choice tree calculation as a normally utilized regulated grouping calculation is regularly connected in rush hour gridlock order, however with the expansion of information volume, the proficiency of C4.5 calculation has been decreased.

Zefan, *et al.*[4], proposed that cuckoo look calculation (CS) is a sort of bionic swarm enhancement algorithm, which is

basic and helpful. In spite of the fact that it has clear points of interest, it can't merge to the ideal arrangement when managing high dimensional complex issues, so its worldwide hunt capacity should be improved. In this paper, opposition-based learning (OBL) methodology and nearby upgraded pursuit are acquainted with improve the essential CS. The former one will be supplanted by the upgraded one if the enhanced one is better. Toward the finish of every age, a potential ideal arrangement will be scanned for locally around the current worldwide ideal arrangement in the advancement bearing. The recreation results demonstrate that the improved calculation improves the worldwide inquiry capacity, union speed and union accuracy of the calculation.

Jabbar, *et al.*[5], said that security hazards in the system develop with increment in size. The assaults on systems have expanded in later past massively and require productive interruption identification frameworks. This paper presents a novel way to deal with group interruption assaults. The focal thought is to apply substituting choice tree (ADT) to interruption information and group the different kinds of assaults. Substituting choice tree is outstanding choice tree calculation utilized for twofold grouping issues. The ADT makes a DT involved forecast hubs what's more, splitter hubs. The ADT calculation is a directed boosting calculation. 2This paper centres to group assaults utilizing ADT. The NSL-KDD Data set is utilized for our test examination. Our proposed technique got a precision of 97.61%, 97.15%, 97.15% and FAR of 3.3, 5.5, 2.38 for DOS, Probe and U2R and R2L individually, which is a lot higher than other existing approaches.

ArunBiradar, *et al.*[8], focused on Mobile Ad Hoc Networks (MANETs) having mobile platforms which has freely mobile. These are self-organizing and adaptive networks. These networks allow the spontaneous formation and deformation of mobile networks. The shortest path problem in MANETS requires that the path from the source node towards destination node be calculated, thereby, minimizing sum of the total costs associated with the path. Some traditional algorithms, such as the Bellman-ford algorithm, the Dijkstra algorithm developed to find the shortest path.

Chetana Khetmal, *et al.*[9], has implemented black hole attack based on AODV, termed as BAODV Routing Protocol. NS2 Simulator is used for simulating MANET [using BAODV, SAODV, MANET, and CBR with FTP by taking 50 nodes]. SAODV is also proposed which is a secure routing protocol that verifies the destination nodes by exchanging the random numbers. SAODV has shown effective prevention of black hole attack (BHA) with better routing efficiency.

Fabrice Le Fessant, *et al*.[10], has focused on sensor networks with environmental monitoring as the main application. The main objective is to bind the effect of separation by the malicious nodes in those networks. The authors has focused on routing protocols which are dependent on tree dependent topology in which the data is send through the sensor node towards sink via tree rooted on the sink. It has been assumed that the routing tree is developed by means of hop distance towards sink. By using periodic routing messages, the routing topology is regularly refreshed. Protocols, namely, RESIST-1 as well as RESIST-0 are analyzed for increasing network resilience by means of sink hole attacks. Risk factor is introduced for measuring the selective forwarding impact.

VII. METHODOLOGY

Routing has always been a challenging task in mobile Ad hoc Networks. A wrongly selected root may lead to an invitation to the intruders. It has been seen often that a miss guided path is more attack prone than that to a well judged path. Trust also seems to be a major point of discussion in the same area. In an ad hoc network, each node in the network must be able to handle the routing of data, which is the domain of the ad-hoc route. As often pointed out, routing is the key question about the ad-hoc network that has been widely discussed by the research community. This article addresses mobile ad-hoc network problems due to lack of infrastructure and dynamic topology. The mobility of these nodes is problematic in terms of mobility management, power consumption, battery life and security. Therefore, these parameters need to be optimized at a minimum cost to design a routing protocol. This research examines in detail the comprehensive review of existing routing protocols and their problems. The presence of malicious nodes in the ad-hoc network can degrade network performance. For the last couple of years, the researchers have paid attention towards development of a safe and secured trust based routing mechanism in order to transfer the data safely. In our research work, an intrusion detection system has been designed to make successful transmission of data. The MANET network has being deployed using 45-60 nodes. There are number of rounds plotted for each node. The intrusion detection system examines each and every node for every round. After this is done, the affected nodes are calculated for all the rounds. Then the intruder node is detected on the basis of the energy consumed by the nodes. The node which consumes maximum energy is labelled as affected node. In case there are two nodes, identified which consume same amount of energy than with the help of another QoS parameter the actual intruder node is identified. Optimization of various QOS parameters such as throughput , delay in ms, bit error rate, energy consumption is performed using Cuckoo search optimization algorithm. The detected intruder is presented using decision tree and removed from the MANET Network.
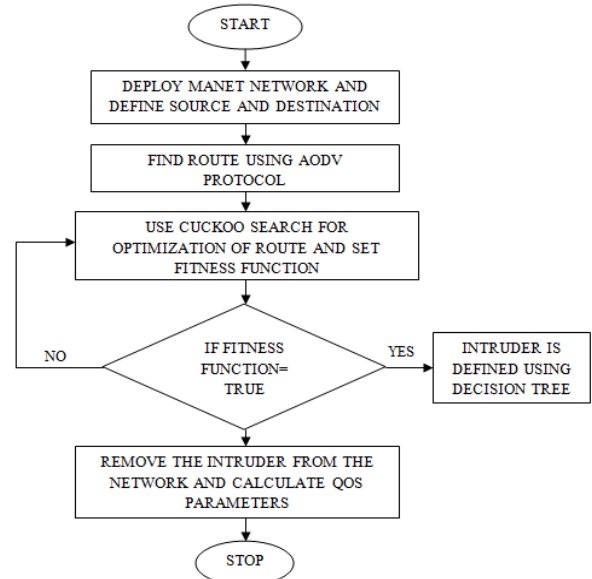

Figure 2. Flow chart of Proposed Work

VIII. RESULTS AND DISCUSSION

Figure 3 shows the network area (MANET) which is designed using MATLAB simulator. It consist of 45-60 nodes with source, destination and attacker node labelled for round 5th. Similarly for each and every round attacker node is identified and among these attacker the node which consumes the maximum energy is the main attacker.
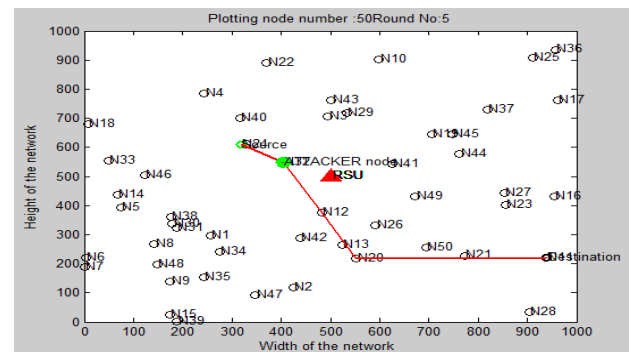

Figure 3. Network Area

Figure 4 represents one of the QoS parameter i.e Throughput. The graph represents enhancement in the throughput parameter before and after optimization using cuckoo search algorithm. Black line shows the value of the throughput before optimization and blue line shows value after optimization.
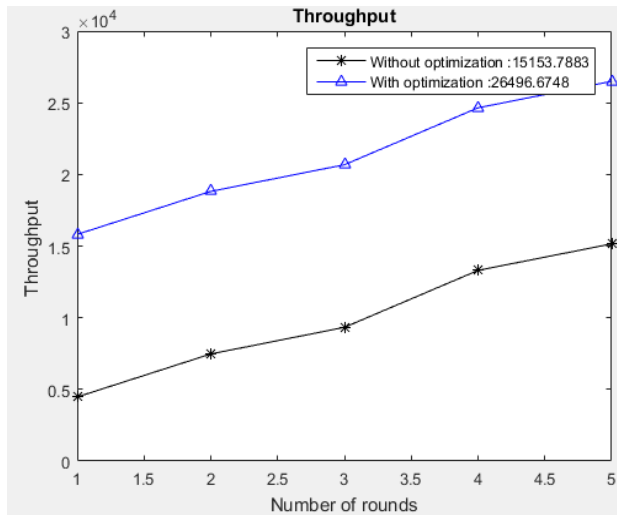
Figure 4. Throughput

Figure 5 represents another QoS parameter i.e Delay. The above graph is plotted for the values of delays obtained while data is transmitted from source node towards destination node. There are two cases which are considered while simulating the code in MATLAB environment. In the first case only AODV protocol is considered whereas in second case delay values are observed when optimization of route is performed by using CS algorithm. From the figure, it is clear that while employing optimization algorithm the delay in the reception of packet has been reduced.
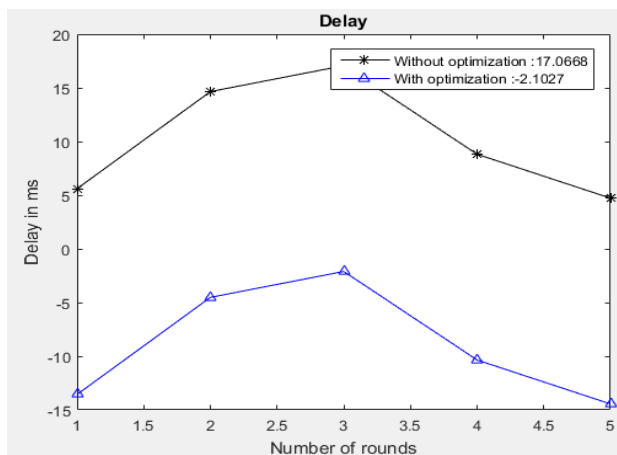

Figure 5. Delay in ms

Figure 6 represents QoS parameter which is set as fitness function for cuckoo search i.e energy consumption. The graph represents reduction in the energy consumption parameter before and after optimization using cuckoo search algorithm. Black line shows the value of the energy consumed before optimization and blue line shows value after optimization.
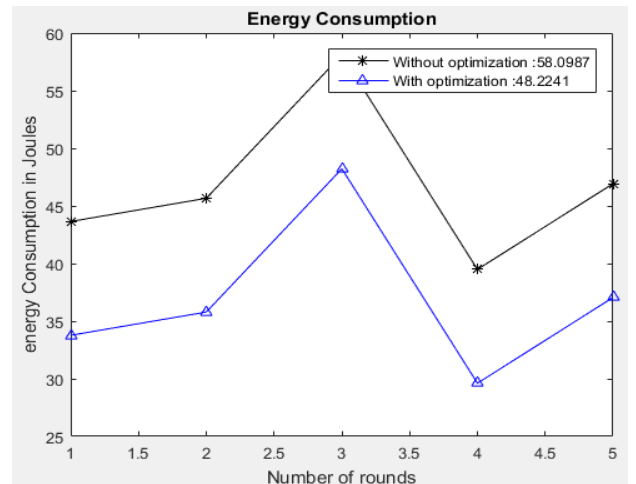

Figure 6. Energy Consumption

The figure 7 represents the BER obtained for the proposed work from the above graph it is clear that BER of the proposed work reduced while using CS in the proposed MANET system. It is clear that the BER is decreased while CS algorithm is used in the network.
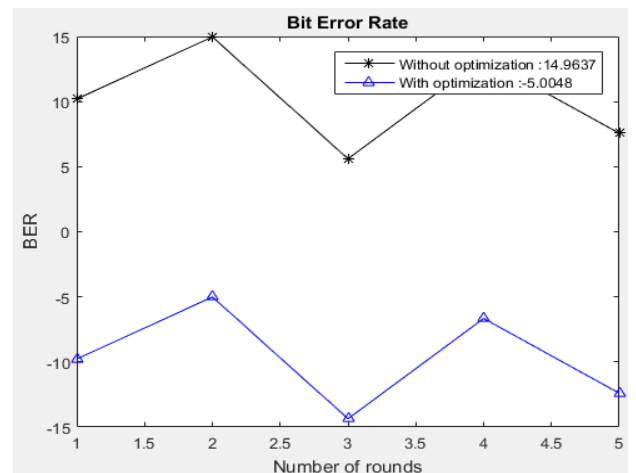

Figure 7. Bit Error Rate

Figure 8 represents the final output in the form of the Decision Tree. X-axis represents the width of the network on which total number of nodes are plotted. Y-axis represents the height of the network. The affected nodes which are identified from each round are also represented. At last Node 21 is labelled as Intruder node and removed from the network.
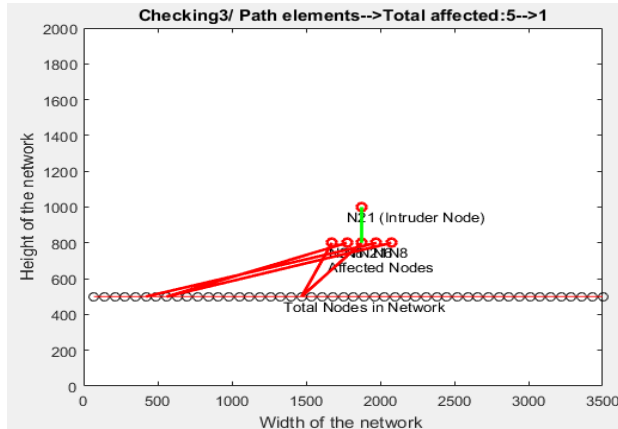
Figure 8. Decision Tree

IX.   CONCLUSION

MANET is made up of individual devices for communication with each other. The concept of the network is no longer familiar with end users with a typical router for sending wireless signals. For network deployment in the Ad hoc network, the developer must consider network configuration. MANETs are popular networks that are widely used because of their nature. Types of networks suffered from various attacks because of no centralized security management. In the proposed work we have mitigated the intrusion in MANET by designing IDS using Cuckoo search algorithm. Optimization algorithm is used for reducing the energy consumption rate, delay as well as bit error rate of the simulated work. AODV routing protocol was utilized for creating the route among source and destination. CS optimization algorithm has been used to optimized the route and find out the intrusion within the route. After this CS algorithm discovered the optimal route for the packet data transmission using its fitness function. The simulations of the proposed mechanism run on MATLAB with 45-60 nodes. After measuring all the parameters, we concluded that the results obtained with CS optimization algorithms are better than the AODV protocol's results. In future, to increase the efficiency of the proposed work neural network or fuzzy logic can be used along with CS algorithm. The features optimized using CS algorithms are used to trained the IDS using machine learning schemes and hence obtained high accuracy.

REFERENCES

[1]   R. Kumari , P. Nand, "*Performance Analysis for MANETs using certain realistic mobility models: NS-2*" , International Journal of Scientific Research in Computer Science and Engineering , Vol. **6**, No. **1**,pp. **70-77, 2018.**

[2]   R. Kumari , P. Nand, "*Performance Analysis of Existing Routing Protocols*" , International Journal of Scientific Research in Computer Science and Engineering , Vol. **5**, No. **5**,pp. **47-50, 2017.**

[3]   P. Rutravigneshwaran, "*A Study of Intrusion Detection System using Efficient Data Mining Techniques*", Int. J. Sc. Res. in Network Security and Communication, Vol. **5**, No. **6**, pp.**5-8, 2017**.

[4]   C.Zefan, Y.Xiaodong, "*Cuckoo Search Algorithm with Deep Search*", In the Proceedings of 2017 3rd IEEE International Conference on Computer and Communications (ICCC 2017),Chengdu, **China**,pp.**2241-2246,2017**

[5]   M.A.Jabbar, S.Samreen, "*Intelligent network intrusion detection using alternating decision trees",* In the Proceedings of 2016 International Conference on Circuits, Controls, Communications and Computing (I4C), Bangalore, **India**, pp.**1-6,2016.**

[6]   A.Hinds, M.Ngulube, S.Zhu, "*A Review of Routing Protocols for Mobile Ad-Hoc Networks (MANET)*", International Journal of Information and Education Technology, Vol. **3**, No. **1**,pp.**1-5,** 2013.

[7]   Z.Yuan, C.Wang, "*An improved network traffic classification algorithm based in Hadoop Decision tree*", In the Proceedings of 2016 IEEE International Conference of Online Analysis and Computing Science (ICOACS), Chongqing, **China**, pp.**53-56**,**2016**.

[8]   A.Biradar, R.C.Thool, "*Effectiveness of Genetic Algorithm In Reactive Protocols For MANET*", International Journal of Engineering Research & Technology (IJERT), ISSN: **2278-0181**, Vol. **2**, Issue **7**,pp.**1757-1761, 2013.**

[9]   C.Khetmal1, S.Kelkar, N.Bhosale, "*MANET: Black Hole Node Detection in AODV*", International Journal of Computational Engineering Research, Vol. **03**, Issue **6**, pp.**79-85,2013.**

[10] F.L.Fessant, A.Papadimitriou, A.C.Viana, C.Sengul, E.Palomar, "*A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis*", Computer Communications ,Vol.**35**, Issue **2**, pp. **234–248**,**2012.**

Authors Profile

Ms. N Kaur studied Bachelor of Technology in Computer science and engineering from Chandigarh University, Mohali (Punjab) in 2017. She is currently pursuing Master of Technology in Computer Science & engineering from Guru Nanak Dev Engineering College, Ludhiana (Punjab). Her main research focuses on development of intrusion detection system using cuckoo search and decision tree to improve performance of MANET.

Mr. K Sharma received a Bachelor degree in Computer Science Engineering in 2011 and a Master degree in Computer Science & Engineering in 2013. He is currently pursuing Ph.D in Computer Science & Engineering. He is with Guru Nanak Dev Engineering College, Ludhiana (Punjab) India as Assistant Professor, in CSE department since 2015- 2019. His research area is data mining and big data.He has published 13 research papers in reputed journals and conferences.