Performance Investigation of Energy Efficiency and provide security in MANETS Using Cluster Selection Algorithm (NS2)

D. GOUSYA BEGUM, M.Tech (Ph.D)
Assistant Professor, Dept. of CSE
S.K .U College of Engineering &Technology
S.K. University, Anantapuramu, A.P

U. DHANUNJAYA, M.Tech (Ph.D)
Assistant Professor, Dept. of CSE
S.K .U College of Engineering &Technology
S.K. University, Anantapuramu, A.P

ABSTRACT :

A Mobile Ad hoc Network (MANET) is a multihopwireless network in which the mobile nodes are dynamicin nature and has a limited bandwidth and minimum batterypower. Due to this challenging environment the mobile nodescan be grouped into clusters to achieve better stability and scalability. In this paper, we consider the various approaches for clustering focus on different performance metrics Specificimplementations of cluster algorithms for application in routingbased on a multi-criteria selection of network parameters areproposed. An efficient BCE cluster selection algorithm [1] based on the combination of important matrices Residual Energy (E), Node connectivity (C) and Available Bandwidth (B) is considered for election of the cluster head efficiently.Hence the security of cluster head is necessary. Here nodes are selected conceding both behaviour based trust value and QoS trust metric values, which leads to a secured and trusted network ,making it highly immune to inside attackers [4] (compromised nodes) and outside attackers. In this paper, we are proposing a trust based clustered algorithm where the trust value is evaluated for every movable devices in the network and the devices with least trust value are discarded as malicious nodes [8].

Keywords:MANET, Reactive Routing, AODV, DSDV, BCE, QoS,IDS.

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) forms a temporary network by comprising some wireless mobile node. It doesn't require the help of any centralized administration or fixed infrastructure. The mobile nodes of MANET dynamically set up paths among themselves which is used to transmit the data temporarily so it is referred as infrastructure less. Otherwise, it is defined as MANET has formed automatically without the help of centralized management or fixed infrastructure by a collection of mobile nodes. Every node in the MANET has both a wireless transmitter and receiver that allow other nodes within its communication range to communicate with each other. Due to frequent changes of mobility and dynamic property of the node in MANET, there may be a huge chance of varieties of attacks such as packet modification, eavesdropping and securing a MANET such conditions is very challenging.Features of mobile ad hoc networks are Wireless channels , Mobile nodes , Applications are military operations, security rescue operations, environmental hazards like earthquake , flooding and hurricane. Routing algorithms of mobile ad hoc networks are mainly classified into two type's namely Proactive routing algorithm or Table Driven and Reactive on demand routing algorithm. In Proactive routing algorithm routing updates and modifications are done dynamically at regular time intervals [7] .

Each node indentifies this changed data and updates in its table. Due to this reason they are also called Table Driven algorithm. Destination- Sequenced Distance Vector (DSDV), Optimized Link-State Routing (OLSR), Topology-Based Reverse Path Forwarding (TBRPF) Protocols are some of the examples.Reactive on demand routing algorithm is used whenever the mobile nodes request for routing process[2]. Some of the examples are Dynamic Source Routing (DSR),Ad Hoc On-Demand Distance Vector (AODV). MANET Applications plays an important role in security, commercially like fire, flood and they can also be helpful to find various features of temperature, pressure and toxins.

II.MOTIVATION

Major challenges of MANET are Error-prone channel state, Hidden problem, Exposed terminals, Bandwidth-constrained, variable capacity links, Energy-constrained operation, Security Issues. Establishing trust among nodes is very important due to security reasons, privacy, and corruption of data and loss of data[10]. In order to enhance the results and efficiency of the Mobile Ad Hoc networks the network is clustered into various subgroups forming clusters depending on

the range of availability of nodes. Cluster heads are selected to communicate among nodes . Suppose if the cluster head itself becomes a malicious node or selfish node, then the routing performance of the entire group communication and network will be hampered. Recently clustered routing algorithm has been proposed . Hence we are proposing a trust based routing algorithm which employs challenging the nodes, rating your friends, friend sharing and route your friends. In this paper we are proposing algorithm for rating and friends sharing [6].

A black hole node hampers the integrity and trust on the network by acting as a healthy node and attracting traffic from the neighboring nodes. It attracts the packets towards itself and drops the data like a 'black hole', which is always ready to absorb any transmission in its surrounding. Hence it deprives the destination and other nodes from data packets. Hence the other nodes keep on waiting for the data from the sender though the sender has already transmitted the data. A compromised node (inside attacker) also called as selfish node is a low energy node [9][11] ,which in an attempt to save its energy deliberately does not involves in communication and hence the data packets sent to that node always experiences drop. As the packets transmitted to it by the other nodes are dropped, it leads to decrease in the rate of energy consumption and hence acts as an idle listener

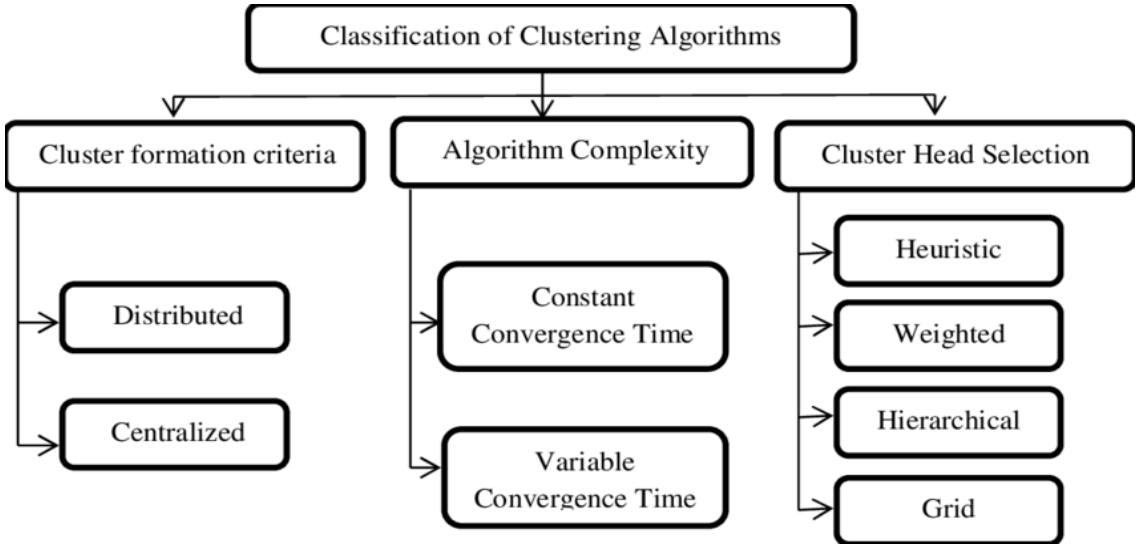

Figure 1: Classification of Clustering Algorithms in MANETS

Insider attackers are of three types-attackers modifying data packets, nodes sending bogus packets (DoS) and selfish nodes (idle listeners with no involvement in communication). Some nodes not detected by IDS, utilize maximum energy in sending bogus packets (DoS)[3][4]. Using our proposed protocol DoS challenges is overcome, by detecting malicious nodes using the Direct Trust value.

III. PROPOSED ALGORITHM

The cluster head selection is done using BCE algorithm.Here the cluster head is selected based on the parameters like residual energy, bandwidth and node connectivity. Based on these three parameters the cluster head is selected. If one of the parameters value is reduced below the threshold value then new cluster head will be elected. The cluster head controls the communication of nodes within the cluster and between other cluster heads of other clusters. Once the cluster head is elected to increase the speed and efficient utilization of bandwidth the multimedia traffic is split using the Top-N rule selection approach algorithm . In this algorithm the data is split depending upon the hit ratio. The shortest path multicast tree is established to send multimedia data to different receivers where the multimedia traffic is split using the Top-N rule selection approach algorithm .Route request phase Let S and D be the source and destination nodes respectively.

Request phase

1) When any leaf node (LNi) contains multimedia data to be transmitted, route discovery is initiated by sending R_REQ . R_REQ message includes destination node address and sequence number.

2) If S contains any route request query from another LNi to the same multicast group and if it contains a valid route to that LNi, it unicasts the R_REQ message (R_REQ+GH address) in the respective GH path. Otherwise S broadcasts the R_REQ.
3) The respective LNi (destination) of multicast tree can only respond to R_REQ message.
4) In case, LNi receives a R_REQ , it rebroadcasts the R_REQ to its neighbors.

Reply phase

1) If LNi receives a R_REQ for a multicast group, it replies with R_REP message if its sequence number is greater than the sequence in R_REQ. R_REP includes the sequence number of multicast group, GH address and hop distance.
2) Note: Hop distance is initially set to zero and incremented for each packet transmission.
3) Also, GH always has rights to send R_REP message to R_REQ message.
4) The LNi or GHi that transmits the R_REP message stores the hop distance of the requesting node before transmitting the reply message.

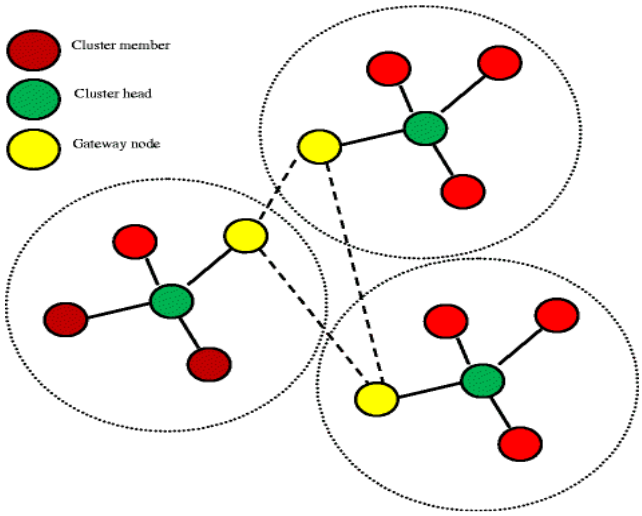

Figure 2: Clustering in MANETS

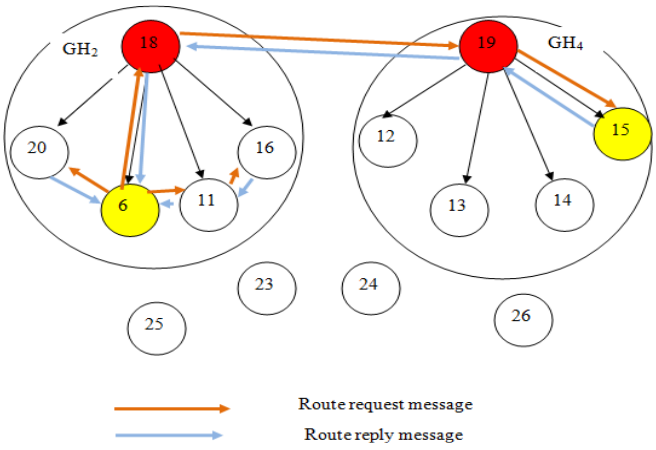

Figure 3: Discovery of Route Establishment

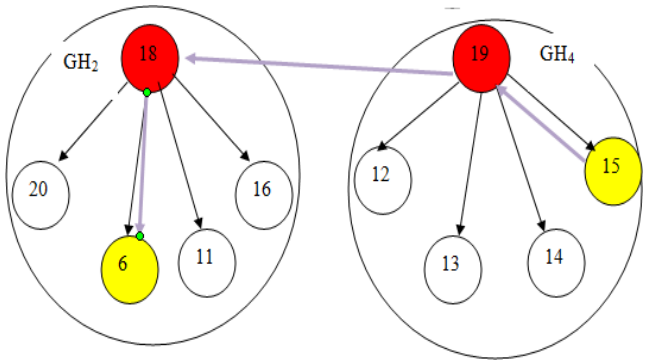

Figure 4: Multicast tree routing using Shortest Path

Hybrid firefly with a genetic algorithm is described in detail for detection of suspicious activity in MANET.Initially, a MANET network is created. The features of black hole attack, gray hole attack, DoS attack, spoofing and selfish misbehaving node and malicious activity node are extracted by proposed hybrid firefly with genetic algorithm technique. The selected features of different attacks are given to RNN classifier that classifies the attacks in MANET. Data Collection Initially, MANET is constructed with 10 nodes. Then the trace files are collected from NS2 which is utilized to detect the attacks on the network. The events occurred in the network is captured by trace files. It contains information like delay in packets, amount of packets transferred from source to destination etc.

Feature selection is used to select more prominent features in the dataset. The feature selection process is processed by proposed hybrid firefly with genetic algorithm technique. It combines both the advantages of Firefly and genetic algorithm. The hybrid approach randomly chooses N features from the attacks. These individual features in the dataset are considered as chromosomes for Genetic Algorithm (GA) or as firefly in the Firefly Algorithm (FA). The proposed hybrid firefly with a genetic algorithm is recovered in two phases for generating the initial population. In genetic algorithm the selection process is used to identify the best parents. Crossover is used to generate the best individuals. Then, based on the fitness value (classification accuracy) N individuals are arranged. Crossover is utilized to generate new N individuals from the selected two chromosomes.

$$C1 = P1 + \mu (P1 - P2)$$

$$C2 = P2 + \mu (P2 - P1)$$

Where μ is a scalar value ranges from 0 to 1. Instead of random mutation operator of genetic algorithm Firefly algorithm is used. Based on the arranged fitness value the global best particle in the population is determined. Divide the N particles into the different position and identify the best position of particles and allocate the particle's neighborhood that provides improved classification accuracy. The effectiveness of the existing Fuzzy based IDS and proposed Hybrid Firefly algorithm-genetic algorithm with RNN (HFA-GA-RNN) is compared in terms of accuracy, precision, and recall. Accuracy is the used to find correctly detected intrusions in all instances. It can be calculated by using the following equation:

$$\text{Accuracy} = \frac{\sum \text{True Positive} + \sum \text{True Negative}}{\sum \text{Total population}}$$

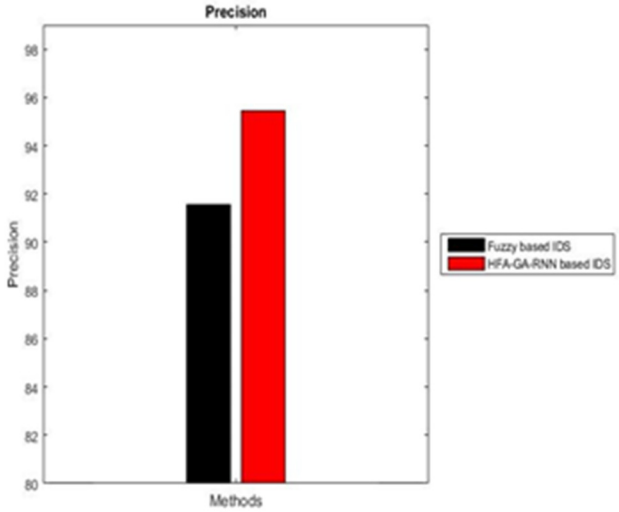

Figure 5. Accuracy Comparison

Figure 5 infersthattheproposedHFA-GA-RNN accuracy is better than Fuzzy based IDS. Here X-axis indicates the methods and Y-axis indicates the Accuracy represented in %.Precision value is evaluated according to the relevant information at true positive prediction, false positive.

$$Precision = \frac{Truepositive}{(Truepositive + Falsepositive)}$$

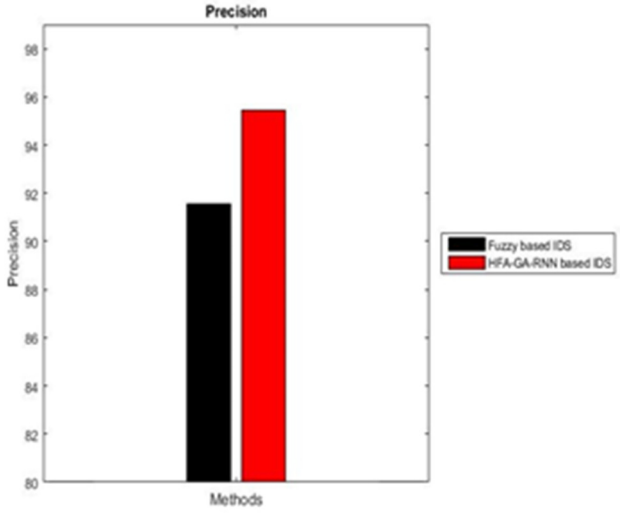

Figure 6. Comparison of Precision

Figure 6 infers that the proposed HFA-GA-RNN Precision is better than Fuzzy based IDS. Here X-axis indicates the methods and Y-axis indicates the Precision represented in %.

IV. CONCLUSION

We have proposed to design Bandwidth Aware Clustering Algorithm. The nodes with maximum residual energy, bandwidth availability and connectivity are chosen as cluster head. Using the cluster head as group leaders and members as leaf nodes, a shortest path multicast tree is established. This helps in transmitting multimedia data to different receivers. Efficient data mining techniques are proposed for Intrusion Detection in MANET A hybrid firefly algorithm with a genetic algorithm is proposed for feature selection of different attacks like black hole attack, gray hole attack,spoofing,selfish misbehavingnode.Thustheproposed method effectively detects the attacks in MANET with better accuracy precision.

REFERENCES

[1]. Saravanan, S., Prabakar, D. and Sathya, S.S., 2023. Trust aware ad hoc routing protocol with key management based mechanism and optimal energy-efficient cluster head selection in mobile ad hoc networks. *Concurrency and Computation: Practice and Experience*, 35 (7), p. e7599.

[2]. Zhang, Y., Liu, L., Wang, M., Wu, J. and Huang, H., 2022. An improved routing protocol for raw data collection in multihop wireless sensor networks. *Computer Communications*, 188, pp. 66 - 80.

[3]. S. S. Muratchaev, A. S. Volkov, V. S. Martynov and I. A. Zhuravlev, "Application of Clustering Methods in MANET," *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, St. Petersburg and Moscow, Russia, 2020, pp. 1711–1714

[4]. K. R. Kambattam, R. Manimegalai, & S. Ganapathy, " An Incremental Feature Selection Approach for Intrusion Detection System in MANET" International Journal for Research in Applied Science & Engineering Technology (IJRASET), vol.5 , pp. 325-329, Jan 2017

[5]. B. Mahapatra and S. Patnaik, "Self Adaptive Intrusion Detection Technique Using Data Mining Concept in an Ad-hoc Network" Procedia Computer Science, 92, pp. 292-297, 2016.

[6]. A. Fidalcastro,E. Baburaj, and M. SaleemBabu, " Detection of attacks on MANET using Sequential pattern mining with feature selection" International Journal of Pharmacy & Technology, Vol. 8, pp. 22937-22950, Dec 2016.

[7]. M. Yoshimachi, and Y. Manabe, "A New AODV Route Discovery Protocol to Achieve Fair Routing for Mobile Ad Hoc Networks", in IEEE 6th International Conference on Information Communication and Management (ICICM 2016), Hatfield, UK, pp. 222-226, Oct. 2016.

[8]. S.D. Kumari, & T. K. Sikamani, " Revival of selfish nodes in clustered MANET" International Journal of Advances in Engineering&Technology,Vol.8,pp.412-419,June2015

[9]. C. Garg, & P. Rewagad, "Analysis of black hole and worm hole attack on AODV routing protocol in MANET" Asian Journal Of Computer Science & Information Technology, Vol.3,pp. 9-12, 2013.

[10]. Sapna B Kulkarni, Yuvaraju BN "ENB Cluster Head Selection Algorithm for MANET", "International Journal on Engineering Technology and Sciences(TM) (IJETS)", Volume-2, Issue-1, and January 30, 2015.

[11]. Sapna B Kulkarni, Yuvaraju BN, "The Top-N rule selection approach algorithm to split the multimedia traffic stream into multiple sub-streams prior to transmission in MANETS", IPASJ International Journal of Computer Science (IIJCS),Volume3,Issue1,January2015