A Mobile Ad hoc Network is always under the threats of different active and passive attacks because of its public access. One of most effective attack in mobile network is the selfish node attack. A selfish node is basically a node that performs all its transmission effectively but not participate as the forwarding node. In this paper, a statistical layered approach is been defined to take the routing decision while excluding the selfish nodes. The work includes the current and short term decision-making. The presented work is effective if the behaviour of nodes changes during the communication. This paper has proposed the algorithm to detect the selfish node over the network.

Key words: Selfish Node, Statistical, Layered Approach.

1. INTRODUCTION

A Mobile Ad hoc Network is a dynamic network that does not require any pre-installed infrastructure such as any centralised controller or the access point. While performing the communication on such dynamic network, routing decision is always a challenge. Another challenge in such network is to achieve the security level. The characteristics that affect the security aspects include the dynamic change in topology, dependency on inherent nodes, no centralize administration etc. Because of this any malicious node can affect and down the whole network. This makes the adhoc network as vulnerable network under different attacks such as spoofing, packet modification, denial of service, eavesdropping etc.

To perform the reliable communication over the network, there is a requirement of some authentication, detection and preventive approaches. The authentication basically includes the verification of the participating node. Authentication of the participating node can be checked using signature matching. The another authentication mechanism is to perform the secure transmission, in such case instead of transferring the data in actual form some cryptographic algorithms are applied on it. In such case, the safety is achieved on the basis of key sharing. Only the authenticated person can derive the actual data. Most of the secure network uses some secure communication mechanism to exchange the information over the network.

Another important aspect of implementing security in MANET is the preventive approach. The preventive communication is basically to identify the safest nodes over the network and perform the communication through these nodes. To perform the preventive communication, the modification in routing algorithm is done. In such communication mode, at first the history based analysis is performed over the neighbouring nodes to identify the high throughput nodes, these reliable nodes are used as the inherent nodes in the network. Generally, the preventive algorithms are not attack specific, they only take the decision based on the communication analysis. Based on this analysis, the next hop selection is done and the communication is performed.

The most widely used solution for different attacks is the detection approach. The detection of the intrusion over the network is done by analysing the attack characteristics. Analysis on each communicating node is performed under the defined set of characteristics. Some of the detection approaches are classified under three main categories called, signature based detection, specification based approach and anomaly detection. As the name suggest, the signature based approaches are the attack specific approach that perform the analysis based on attack definition. The effects of particular attack are analysed over the network to perform the intrusion detection. Once the detection is performed, the node is detected as the misbehaving node and the communication is performed after excluding the attacker node. Another kind of detection approach is the specification based approach. In such kind of approaches, the limitation of the attack is analysed. In such approach, the correct communication analysis for the critical objects is analysed under the security specification. Such kind of systems are implemented for privileged programs, applications or the protocols. Based on the analytical study, most appropriate communicating nodes are identified for the communication.

The third and important categorization of detection approaches is anomaly detection. The analysis is performed on the communication activity. The complete available activity statistics is divided in two parts called training data and testing data. The training data where defines the existing communication with
decision. The testing data is the current communication that is required to be analyzed. This approach gives the decision based on the statistical or mining based analysis. The significance of this approach is the detection of unknown attacks. Different kinds of attacks under selfish node are defined as under:

2. RUSHING ATTACK
The rushing attack is the suppression operation performed by a node to increase the duplicate communication. This kind of communication actually floods the network to perform the route discovery so that the effective route can be identified. When the source node flood the network to discover the appropriate route, each intermediate node will be process more then once. So that lot of duplicate request packets are transmitted by the selfish node. The attacker node does not taking care of other communication performing over the network and exploits itself as the high priority node.

3. BLACKHOLE ATTACK
A black hole node is node that accepts the data from other nodes as the receiver node or the intermediate nodes but does not forward it to the next node. It drops all the forwarding packets in the routing path. This kind of selfish node results in very low packet delivery ratio.

4. NEIGHBOUR ATTACK
This kind of selfish node forward the packet to the node but does not store the communicating information such as the ID of the sender or receiver node. If some communication fails, this kind of attacks cannot help to troubleshoot the communication effect.

In this paper, a layered approach for the detection of selfish node is defined. In this section, the introduction to manet, manet security challenges and the different attacks under selfish node attack are described. In section II, the work done by earlier researchers in same area is discussed. In section III, the work proposal is described along with algorithmic approach. In section IV, the conclusion derive from the paper is described.

5. LITERATURE SURVEY
S.Lakshmi present an adaptive selfish aware queue scheduler for a M/M/1 and M/M/n queuing mechanism to schedule the packets for selfish nodes in mobile ad hoc networks using AODV as the routing protocol[1]. Sivaranjani V performed a work on secure approach for cluster head selection in case of selfish node. In this paper, Leader election is studied in the presence of selfish node for intrusion detection in Mobile Ad Hoc Networks (MANETs). To balance the resource consumption among all the nodes, the most cost-efficient leaders with the most remaining energy must be elected as leader. But, the selfish nodes may behave selfishly by lying about their energy level and avoid them being elected[2]. Djamel Djennouri propose in this paper a novel cross-layer based approach to detect data packet droppers, that Author optimize and decrease its overhead. Contrary to all the current detective solutions, ours is applicable regardless of the power control technique employment[3]. Hadi Otrok address the problem of increasing the effectiveness of an intrusion detection system (IDS) for a cluster of nodes in ad hoc networks. To reduce the performance overhead of the IDS, a leader node is usually elected to handle the intrusion detection service on behalf of the whole cluster[4]. K. Paul detect a large range of attacks on Dynamic Source Routing (DSR) protocol. Author provide a low-cost mechanism informing other nodes of the system about the accused and provide an inference scheme to blame the accused and malicious accuser without doubt[5].

Hanif S. Kazemi present the design and implementation of a distributed network monitoring system for MANETs. Presented system is completely distributed, generates no additional traffic on the network and produces a dynamic picture of the network level and node level information on a graphical user interface. In Presented proposed scheme, multiple monitoring nodes collaborate to achieve a reasonably accurate snapshot of the network conditions[6]. Thomas Lochmatter investigate the problem of detecting selfish and malicious nodes in a hybrid multi-hop network by the operator. The setup Author consider consists of an ad-hoc multi-hop network which is connected to a central trusted authority (operator) through a base station[7]. Sunil kumar S. Manvi proposes routing misbehavior detection in MANETs using 2ACK scheme. Routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. Author simulated the routing misbehavior detection using 2ACK scheme to test the operation scheme in terms of performance parameters[8].

Frank Kargl will analyze the detection mechanisms proposed by others. Presented new detection mechanisms that Author describe in this paper are called activity-based overhearing, iterative probing, and unambiguous probing. Simulation-based analysis of these mechanisms show that they are highly effective and can reliably detect a multitude of selfish behaviors[9]. Preeti Nagrath discusses reputation based schemes that can be applied to ARAN to detect selfish node and improve the performance[10]. E.Venkat Reddy presented the benefits of routing protocols. The implementation of this protocol is made on the network layer based on the Dynamic Source Routing (DSR) protocol. Author present a performance analysis of DSR fortified by RMP and compare it to regular defenseless DSR. A network with RMP is observed to improve about 60% of misbehaving nodes in the network, in contrast to a defenseless network[11]. Hugo Miranda performed a work on prevention approach in case of selfish node. Mobile ad hoc networks are a new and challenging topic on mobile computing. A particular characteristic of ad hoc networks is their self-organization, what makes them highly dependable of the participants[12].

Yanchao Zhang propose SIP: A Secure Incentive Protocol to stimulate cooperation among those possible selfish nodes. The most attractive feature of SIP is that it does not rely on any predefined infrastructure and provides highly secure incentives for selfish nodes to be cooperative in packet forwarding with low overhead and implementation complexity[13]. Zougagh Hicham performed a comparative study of intrusion detection in adhoc network. In recent years, the use of mobile ad hoc network (MANETs) has been widespread in many applications.
Due to its deployment nature, MANETs are more vulnerable to malicious attack. The absolute security in the mobile ad hoc network is very hard to achieve because of its fundamental characteristics, such as dynamic topology, open medium, absence of infrastructure, limited power and limited bandwidth. In this article, the author classifies the architecture for IDS that have so far been introduced for MANETs, and then existing intrusion detection techniques in MANETs are presented and compared. The author then provides some directions for future researches [14]. Aishwarya Sagar Anand Ukey defined a new reputation based approach is proposed that deals with such routing misbehavior and consists of detection and isolation of misbehaving nodes. The proposed approach can be integrated on top of any source routing protocol and based on sending acknowledgement packets and counting the number of data packets of active path [15]. Isha V. Hatware compares the behavior of three routing protocols DSDV, DSR and AODV, with the consideration of the node misbehavior. This problem of node misbehavior can be detected and controlled by different techniques such as Intrusion Detection System (IDS), Cooperative Intrusion Detection, watchdog and path rater discussed in this paper which are more efficient than other general techniques [16]. Bo Wang presents an adaptive on-line algorithm to detect such selfish behavior based solely on local observations of messages exchanged by AODV-like routing protocols. The author uses a finite state machine model of locally observable protocol actions to generate a statistical description of the behavior of each neighbor and apply statistical analysis to cluster neighboring nodes on the basis of behavioral similarities and identify the selfish ones. Through simulation, the author evaluates the performance of the presented method with respect to the probability of detecting selfish nodes and the rate of false positives against two generic selfish strategies—dropping route requests and dropping route replies [17]. Tiranuch Anantvalee author classifies the architectures for intrusion detection systems (IDS) that have been introduced for MANETs. Current IDS’s corresponding to those architectures are also reviewed and compared. The author then provides some directions for future researches [18].

### 6. PROPOSED ALGORITHM

The presented work is about to identify the selfish node over the network by performing a statistical analysis on neighboring nodes. This algorithm is capable of identifying the reliable route over the network. In this work, a layer approach is defined to perform a long-term analysis and short-term analysis. The short-term analysis is performed on neighboring nodes under different parameters. The basic architecture of the analysis is described in Figure 1.

As we can see, the first layer is described by short-term analysis. The parameters considered in this layer are shown in Figure 2.

Once the next hop communication parameters are derived, the next work is to perform the decision making for the selection of nodes. Based on these parameters, the priority will be assigned to these nodes. The node having the higher packet delivery ratio is having the higher priority. The second level parameters include the delay rate and the response time analysis. The hop with minimum delay and minimum response time will be considered as the effective communicating nodes.

Once the high-level communication will be drawn, at second level, aggregative analysis will be performed. This is the long-term analysis in which the communication statistics analysis will be performed based on the communication performed till now. The parameters considered in this work are the loss rate analysis, the throughput analysis, and forwarding rate analysis. These parameters are described in Figure 3.
The presented work is described in the form of a flow chart shown in Figure 4.

![Flow Chart](chart.jpg)

7. CONCLUSIONS
In this paper, a layered approach is presented to identify the selfish node over the network. The work is divided in two main phases first to perform the current communication analysis and other to perform the history based analysis. The work will identify a reliable route and avoid the selfish node as the intermediate node.

REFERENCES