Energy Efficient usage of Intrusion Detection System in MANET

Sureka. M[1]**, Kalaivani. K**[2]**,**

[1,] *Student Member, Department of Computer Science and Engineering,*
[2]*Staff Member, Department of Computer Science and Engineering, Arasu Engineering College – Kumbakonam, TamilNadu, India.*

Abstract

Mobile Adhoc Networks (MANET) is self-configuring, infrastructure less, dynamic wireless networks in which the nodes are resource constrained. Intrusion Detection Systems (IDS) are used in MANETs to monitor activities so as to detect any intrusion in the otherwise vulnerable network. The existing method is based on reduce individual active time of the IDS although it consumes higher energy one of the main difficulties face it's in an existing system is security problems. So proposed system demonstrates the implementation of network security algorithms can significantly reduce their energy consumption compared to the existing system. The paper has the main contributions (i) a new feature extraction algorithm with low processing demands (ii) a feature selection method with two objectives - accuracy and energy consumption. The new feature extractor demands significantly less computational power, memory, and energy. So in this paper presented an original solution called VFDT (Very Fast Decision Tree) it has a new set of techniques to improve the energy efficiency in anomaly based packet classification, using machine learning algorithms. Proposed system focus on the practical details of feature selection and extraction, and compare the energy efficiency using IAPCMAC protocol of several SW implementations.

Keywords**:** IDS, Energy efficiency, VFDT, MANET, IMAPC MAC protocol.

I. INTRODUCTION

A mobile ad hoc network (MANET) is self-configuring infrastructure less network of mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose". Each device in a MANET is free to movie independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger internet. MANETs are kind of wireless ad hoc network that usually has a routable networking environment on top of a link layer ad hoc network.

Security in Mobile AdhocNetwork

A lot of research has been done in the past but the most significant contributions have been the PGP (Pretty Good Privacy) and trust based security. None of the protocols have made a decent trade off between security and performance. Is an attempt to enhance security in protocols and some of them have suggested new protocols.

Attack Classifications in Mobile Adhoc Network

These attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing.

1. *Application Layer: Malicious code, Repudiation*
2. *Transport Layer: Session hijacking, Flooding*
3. Network Layer: Sybil, Black & Grey hole, Spoofing
4. *Data Link/MAC: Malicious & Selfish behaviour, Active*
5. *Physical: Interference, Eavesdropping*

Intrusion detection system

Network intrusion detection systems are most efficient way of defending against network-based attacks aimed at computer systems. These systems are used in almost all large-scale IT infrastructures. Although several IDS systems are available, the common objectives of these systems are to reduce the amount of false alarms, and to recognize new attacks in order to increase detection ratio. In this paper, the concentration is on detecting known and unknown attacks in fast networks in order to mitigate the influence of the attack by shrinking the time gap between the real attack and its detection.

1. Signature Based Detection
2. Anomaly Based Detection

The contributions of this project are summarized as follows:

The proposed system is dedicated to detect intrusions on a network by using anomaly intrusion detection approach. This approach is used to detect the known and novel attacks in traffic network.VFT(very fast decision tree) algorithm is selected as classifier to achieve this goal because it is capable of processing and analysing of high-speed network traffic, and detecting the intrusion in real time. The features are extracted from each network packet. The proposed system consists of two phases. The feature extraction phase starts with the selection of the desired kind of traffic by filtering the network packets based on protocol fields or flags, patterns of bits, or packet content. The feature selection process identifies the most relevant features from a feature set, aiming at improving the classifier accuracy and reducing the computational load during classification. The features are organized:

(i)Header-based(features extracted directly from each packet header)

(ii)Host-based(features extracted from the general communication history or data flow between two hosts) and

(iii)Service-based(extracted from the communication history between two hosts, and specific to a single service)

II. RELATED WORKS

Sunil Kim et al pattern matching is one of critical parts of Network Intrusion Prevention Systems (NIPS) [1]. Pattern matching hardware for NIPS should find a matching pattern at wire speed. However, that alone is not good enough. First, pattern matching hardware should be able to generate sufficient pattern match information including the pattern index number and the location of the match found at wire speed. Second, it should support pattern grouping to reduce unnecessary pattern matches. Third, it should guarantee worst case performance even if the number of patterns is increased. Finally it should be able to update patterns in a few minutes or seconds without stopping its operations. In propose system architecture to meet the above requirements. Using Xilinx FPGA simulation, This paper show that the new system scales well to achieve a high speed over 10Gbps and satisfies all of the above requirements.

Vijayasarathy et al denial of service attacks poses a big threat to any electronic society. DoS and DDoS [2] attacks are catastrophic particularly when applied to highly sensitive targets like Critical Information Infrastructure. While research literature has focused on using various fundamental classifier models for detecting attacks, the common trend observed in literature is to classify DoS attacks into the broad class of intrusions, which makes proposed solutions to this class of attacks unrealistic in practical terms. In this work, the approach to a carefully engineered practically realized system to detect DoS attacks using a Nave Bayesian (NB) classifier is described. The work includes network modeling for two protocols TCP and UDP.

Fitaci et al assume that the network in divided into clusters of nodes [3] among which some are trusted. A trusted node is equipped with perfect IDS so that when it performs intrusion detection, it is effective for the whole cluster and no other node is involved in the monitoring process. In comparison, the proposed approach neither assumes that some nodes are trusted nor that an IDS is perfect. This work assume the network to be static while the proposed approach works even when the nodes are mobile.

Tsikoudis et a1 presented for network-level intrusion detection system which resolves the energy-latency [4] trade-off by providing both low power consumption and low detection latency at the same time. Packet-based selective encryption is used for reducing the energy consumption during intrusion detection for networked control systems security.

III. METHODOLOGIES

The proposed system is dedicated to detect intrusions on a network by using anomaly intrusion detection approach. The goal of an Intrusion Detection System (IDS) is to identify security violations in a computing system. A Network Based Intrusion Detection System (NIDS) monitors the traffic by analysing packets, hosts, and service flows in search of attacks.

The main aim of this proposed system is

1. The proposed intrusion detection system can cope with fast networks.
2. The proposed IDS are to reduce the amount of false alarms and to recognize new attacks in order to increase detection ratio and system operates in two grains levels.
3. The new feature extractor consumes low energy used by a commercial tool, when implemented in software.

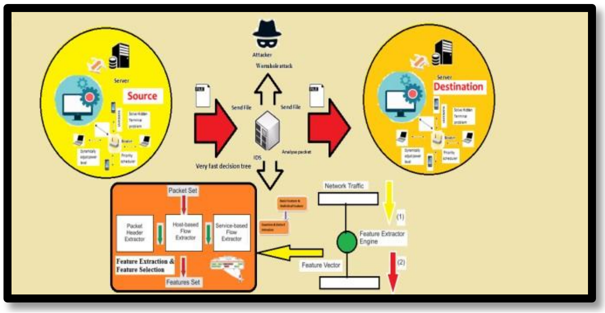


Figure 1: Energy Efficiency usage of Intrusion Detection System in MANET

The main contribution of this project is summarized as follows:

The proposed system is dedicated to detect intrusions on a network by using anomaly intrusion detection approach. This approach is used to detect the known and novel attacks in traffic network.VFT(very fast decision tree) algorithm is selected as classifier to achieve this goal because it is capable of processing and analysing of high-speed network traffic, and detecting the intrusion in real time.

Feature Extraction

The feature extraction phase starts with the selection of the desired kind of traffic by filtering the network packets based on protocol fields or flags, patterns of bits, or packet content.

Feature Selection

The feature selection process identifies the most relevant features from a feature set, aiming at improving the classifier accuracy and reducing the computational load during classification.

The main objectives of the system is

1. To detect the intrusion in the MANET.
2. To reduce the energy consumption without degrading the quality of sending packets.

Considerable saving in energy and computational cost is achieved using the proposed technique of optimizing the active time of the IDSs while maintaining the performance of the IDS.

0verall, there are three modules in our proposed system to detect intrusions on a network, including AODV Routing, Intrusion Detection, IMAPC MAC Protocol(Saving energy), Performance Evaluation .

A. AD-HOC On-Demand Distance Vector Routing (AODV) Protocol

AODV is an on-demand routing protocol designed for operation of mobile ad hoc network. Protocol provides self starting, dynamic, loops free, multi-hop routing. Protocol allows mobile nodes to establish routes quickly for new destinations as well as to respond to changes in network topology and link failures as only affected set of nodes are notified. Nodes do not maintain routes to the destinations that are not in active communication. New routes are created on demand. It means control packets are broadcast when needed and hence eliminate the need for periodic broadcast of routing updates.

AODV protocol works in two phases,

a) Route discovery process and

b) Route maintenance process.

Route discovery process uses Route Request (RREQs) and Route Reply (RREPs) messages. The routing messages contain information only about the source and the destination. When a route to destination is needed, the node broadcasts a route request (RREQ) packet to its neighbours to find the optimal path.

RREQ message contains route request broadcast ID, Destination IP Address, Destination Sequence Number, Source IP Address, Source Sequence Number and Hop Count. Sequence number is used for route freshness, loop prevention and faster convergence. When a node sends any type of routing control message like RREQ/RREP, it increases its own sequence number. Every node should include the latest sequence number for the nodes in the network in its routing table. It is updated whenever a node receives RREQ, RREP or RRER related to a specific node. Hop count represents the distance in hops from the source to destination. Each node receiving the RREQ message sets up reverse path back to the sender of the request so that RREP message can be unicast to that sender node from the destination or any intermediate node that satisfy the request conditions.

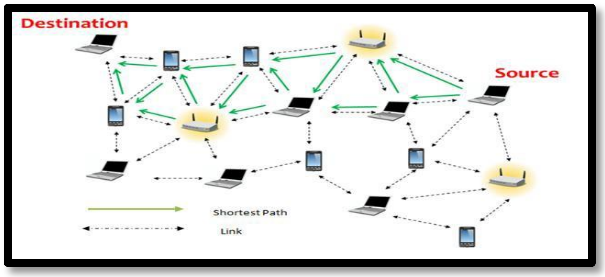


Figure 2: The routing message exchange in AODV

Upon receiving the route request message, the intermediate node forwards the RREQ message until a node is found that is the destination itself or it has an active route to the destination with destination sequence number greater than or equal to that of RREQ. This node replies back to the source node with a route reply message RREP and discards the RREQ. If the intermediate node receives RREQ with 'G' flag set, it must also uncast gratuitous RREP to the destination node. RREP contains Destination IP Address, Destination Sequence Number, Originator IP Address and Lifetime. Forward links are setup when RREP travels along the reverse path. Once the source node receives the route reply, it establishes a route to the destination and sends data packet along forward path set-up.Route maintenance is performed with two additional messages: Hello and RRER messages. Each node broadcast Hello messages periodically to inform neighbours about its connectivity. The receiving of Hello message proves that there is an active route towards the originator. When a node does not receive HELLO message within time period from a neighbour node then it detects that a link to that neighbour node has broken then it generates route error message (RRER). RRER message indicates those destinations that are unreachable, their IP address and destination sequence number. In order to inform the link failure information, each node maintains a precursor list for each routing table entry containing the IP address of set of neighbouring nodes that are likely to use it as a next hop towards each destination. On receiving this RRER, each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. In addition to these routing messages, the route reply acknowledgment (RREP-ACK) message must be sent by sender node of RREQ in response to a RREP message with the 'A' bit set. This provides assurance to the sender of RREP that the link is bidirectional.

B. Intrusion Detection

Consider a network of wireless nodes, each having an intrusion detection system (IDS) that is responsible for detecting malicious activities within its neighbourhood. Assume that a mobile node is watched for malicious activities by all its neighbours (nodes within its radio range) using these IDSs. Hence, by neighbour, i.e., 1- hop neighbour throughout the rest of the paper. At any instant of time, all or some of the k neighbours may detect the malicious activity of node a depending upon the detection rate of the IDS components on them.

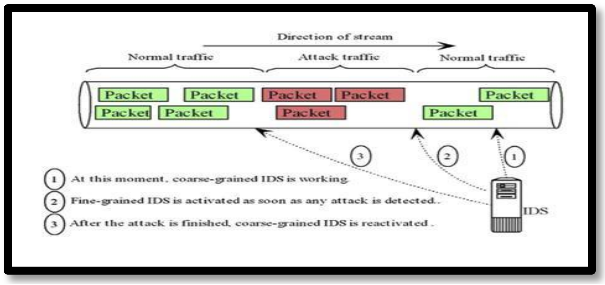

Direction of stream
Normal traffic
Attack traffic
Normal traffic
Packet
Packet
Packet
Packet
Packet
Packet
Packet
Packet
Packet
3
2
1
1 At this moment, coarse-grained IDS is working.
2 Fine-grained IDS is activated as soon as any attack is detected..
3 After the attack is finished, coarse-grained IDS is reactivated .
IDS

Figure 3: Detection of Intruders in Fine-grained IDS

VFDT is a high-performance data mining system based on Huffing trees. Many of classification learning methods have been proposed, of which the decision tree learning method is commonly used. This is because it is fast and the description of classifiers that it derives is easily understood. One of the data stream algorithms that support the decision tree learning method is the VFDT. As data arrives, this data stream grows gradually while the data is classified. VFDT allows the use of either information gain or the Ginny index as the attribute evaluation measure. It includes a number of refinements to the algorithm.

```
Algorithm: VFDT(S,X,G,  )
Input: S is a sequence of vector of features, X is a set of discrete attributes, G(.) is a split evaluation function,    is one minus the desired probability of choosing correct feature at any given node.
Output: HT is a decision tree
Begin:
        Step 1: Let HT be a tree with single leaf    (the root  )
        Step 2: Let    =X U{    }
        Step3: Let    (    ) be the G obtained by predicting the most frequent class in S.
        Step 4: For each class
        Step 5:   For each value      of each attribute        X
        Step 6:        Let      (   )=0
        Step 7: For each example (x,    ) in S
Step 8: Sort (x,y) into a leaf using HT
Step 9: For each in X such that
Step 10: Increment ( )
Step 11: Label with the majority class among the examples seen so far at
Step 12: If the examples seen so far at are not all of the same class, then
Step 13: Compute Ġ1( ) for each attribute - { }
Step 14: Using the counts ( )
Step 15: Let be the attribute with highest
Step 16: Let be the attribute with second highest
Step 17: Compute = ———— / 2n
Step 18: If ( )- ( ) and
Step 19: Replace by an internal node that splits on
Step 20: For each branch of the split
Step 21: Add a new leaf , and let = X-{ }
Step 22: Let ( ) be the Ġ obtained by predicting the most frequent class at
Step 23: For each class and each value of each attribute - { }
Step 24: Let ( ) = 0
Step 25: Return HT
End…….
```

C.IMAC-MAC Protocol

Improved autonomous power control MAC protocol the proposed system is used and improve the energy level. Scheduling is used to exchange packet between sources to destinations.

1. Pre-emptive
2. Non pre-emptive

1) Estimation of Power Level:

$$E_s = \text{———} \qquad t_s, t \geq o, p > 0$$

Where,

T_p - Transmit the total packet.

R_p -Receiving packet from source.

D_p - Retransmitting the packet.

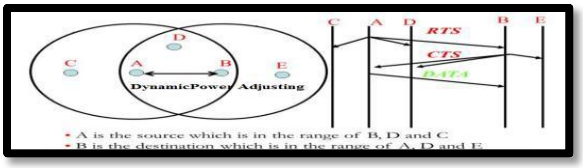

C
A
D
B
E
RTS
CTS
DATA
D
C
A
B
E
DynamicPower Adjusting
• A is the source which is in the range of B, D and C
• B is the destination which is in the range of A, D and E

Figure 4: IAPCMAC protocol dynamically adjust the power level between the nodes

2) Power utilization:

$$\text{—} = \text{————} * \beta(OP)$$

Where,

- Total number of successful data bits sent between source and destination - Total energy consumption in the network

N - Total number of packets sent(including control packets) for duration of the simulation (from all nodes).

3) IAPCMAC Protocol:

Power saving schemes has been proposed to minimize energy consumption in MANETs. These schemes fall under three main categories:

- Transmission power control
- Low power mode
- Power saving

4) Transmission Power Control:

Transmission power control is adjusted according to desired criterion. Power conservation is to reduce the amount of power used by individual nodes and by the aggregation of all nodes to transmit data through the ad hoc network. Two components determine the cost of communication in the network. First one is direct node to node communication or transmission. The transmission rate can be adapted by the sender. Second is forwarding of data through the networks. In the first case we can use the power control techniques to conserve the power. Whereas in the second case we can use the energy efficient power control scheme.

Current technology supports power control by enabling the adaptation of power levels at individual nodes in an ad hoc network. Since the power required transmitting between two nodes increases with the distance between the sender and the receiver, the power level directly affects the cost of communication. The power level defines the communication range of the node and the topology of the network. Due to the impact on network topology, artificially limiting the power level to a maximum transmit power level at individual nodes is called topology control.

5) Low Power Mode:

IAPCMAC, an energy-conserving multi-access protocol for MANETs using busy tones where radios that are not actively transmitting or receiving a packet power themselves off in a manner that does not influence the delay or throughput characteristics of the protocol.

The node with the goes to idle state and it is considered as an off state, such as the power level not decrease. This protocol only saves power with increasing the overall network throughput.

6) Power Saving:

1. ON/OFF mechanism of nodes: In this, any node can power off itself when there is nothing to do for that node or if any neighbouring node is transmitting at that time. A node can power down itself for without affecting the performance of neighbour nodes.

2. Power saving mechanism: In this, control messages are sent using maximum power available and data messages are sent using minimum or sufficient power required for transmission.

7) Optimum Transmission Power:

Calculate the optimal values for the following: OP = ( ) *

packets, the queue length of Y(MP) and Z(LP) may increase
Where,

OP - Optimal value of transmission power
- Optimal transmission time
- Optimal transmission rate

8) Scheduling Phase:

This priority scheduling gives each process a priority well defined. This way every process has its own priority on which will depend if it is going to be run or wait. The first one to run is going to be the process with highest priority, while others will wait for their turn. It schedules the data packets based on its priority index. The priority index is attached to the header of the data packets. Its value is based on the queue length of the node, data rate of the source (which is normalized with respect to channel capacity), and expiry time of the packet. This scheduler favours data packets as compared to control packets. It aims to improve the average throughput by quickly delivering packets with greater remaining hops or distance.

9) Priority Queue:

Priority queue is for selecting flows based on the priority. Here the priority is assigned for flows which contain loss number of slots, optimal transmission rate of flow and optimal transmission power of flow. All the flows are queued based on the priority. The flows are entered into the queue based on the priority which they have

The flows will be queued based on their priorities. After getting the input priorities queue we will apply the non-pre-emptive scheduling algorithm. We will get the optimal transmission rate value and the optimal transmission power value.

10) Calculate the queue length:

The percentage of Queue length α, β, and γ for X, Y and Z queues respectively are calculated as in following equation,

$$\alpha = \underline{\qquad\qquad\qquad}$$

$$\beta = \underline{\qquad\qquad\qquad}$$

$$\gamma = \underline{\qquad\qquad\qquad}$$

Where,

- Queue length of X (HP – Higher priority)
- Queue length of Y (MP – Medium priority)
- Queue length of Z (LP – Lower priority)

We decide the number of packets to be each queue based on their access ratio given in equation
$w0\alpha : w1\beta : w2\gamma$
Where,

w0, w1, w2 are the user defined weights assigned for X(HP), Y(MP) and Z(LP). α is the percentage of X(HP) packets, β is the percentage of Y(MP) packets and γ is the percentage of Z(LP) packets waiting in their respective queues. When the traffic is dominated by Y(MP) or Z(LP) and thus the access ratio of X(HP) packets.

IMAPC-MAC Protocol Algorithm

1. Start
2. Define $P_i=\{P_1,P_2,P_3\ldots\ldots\ldots P_n\}$ (set of flow),
   $Q[P_i]$ = priority queue
3. N – Number of packet allocated for each flow
4. Calculate the queue length using by the non-pre-emptive technique
5. Transmitter power is estimate using priority scheduling
6. Add that flow to the queue $Q[P_i]$
   OP = ( ) *

Where,

OP - Optimal value of transmission power
- Optimal transmission time
- Optimal transmission rate

7. Transmission cycle is finished.
8. End

IV. PERFORMANCE EVALUATION

In this section we discuss Algorithm VFDT, Improved autonomous power control MAC Protocol in MANET performance.

A. Throughput:

It is defined as the total number of packets delivered over the total simulation time.
Mathematically, it can be defined as:

✓ Throughput=Number of packet/Processing time

✓ Energy operation= - * processing time

Where,

N is the number of bits received successfully by all destinations.

B. End to end delay:

The average time it takes a data packet to reach the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination. Mathematically, it can be defined as,

Avg. EED=S/N

Where,

S is the sum of the time spent to deliver packets for each destination,

N is the number of packets received by the all destination nodes.

C. Packet delivery ratio:

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. Mathematically, it can be defined as:PDR= *S1*÷ *S2*

Where,

S1 is the sum of data packets received by the each destination.

S2 is the sum of data packets generated by the each source

TABLE I
AVERAGE ENEGRY CONSUMPTION FOR THE EXTRACTION OF EACH FEATURE

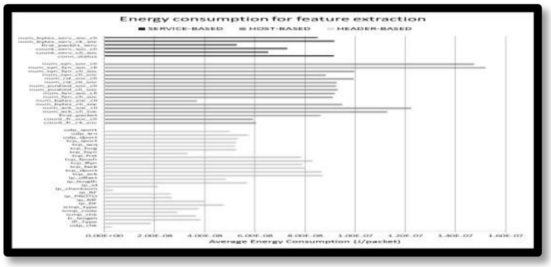
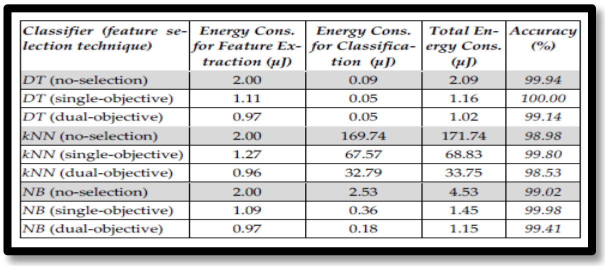
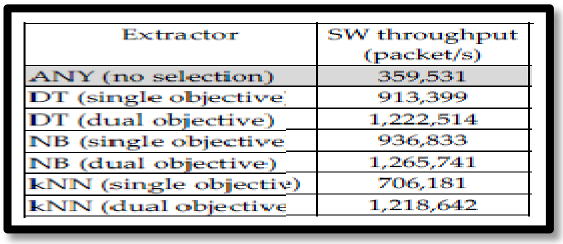


TABLE II
COMPARSION OF ENEGRY CONSUMPTION FOR FEATURE EXTRACTION ENGINE AND ML CLASSIFIERS



Classifier (feature selection technique)	*Energy Cons. for Feature Extraction (μJ)*	*Energy Cons. for Classification (μJ)*	*Total Energy Cons. (μJ)*	*Accuracy (%)*
DT (no-selection)	2.00	0.09	2.09	*99.94*
DT (single-objective)	1.11	0.05	1.16	*100.00*
DT (dual-objective)	0.97	0.05	1.02	*99.14*
kNN (no-selection)	2.00	169.74	171.74	*98.98*
kNN (single-objective)	1.27	67.57	68.83	*99.80*
kNN (dual-objective)	0.96	32.79	33.75	*98.53*
NB (no-selection)	2.00	2.53	4.53	*99.02*
NB (single-objective)	1.09	0.36	1.45	*99.98*
NB (dual-objective)	0.97	0.18	1.15	*99.41*

TABLE III THROUGHPUT OF THE EXTRACTOR



Extractor	SW throughput (packet/s)
ANY (no selection)	359,531
DT (single objective	913,399
DT (dual objective)	1,222,514
NB (single objective	936,833
NB (dual objective)	1,265,741
kNN (single objectiv)	706,181
kNN (dual objective	1,218,642

V. **CONCLUSION**

Therefore from the analysis of above result it is cleared that proposed system is more suitable and efficient to be implemented in MANETS. As in this proposed system there is slight increase in the routing overhead. In future, to enhance the performance of the mobile adhoc networks more effectively. Security is the important issue of routing protocols of MANET. Mobile adhoc network has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. Proposed system that detects and prevent the wormhole attack using appropriate measures based on the cluster head relationship with other cluster heads. And also tries to mitigate the impact of the attack by using the intrusion detection system. Overall this paper promises improvement of overall throughput by increasing packet deliver ratio and reducing mobility and flooding. It can be fastest growing area for future research in terms detection techniques, response mechanism and selection of nodes feature for data collection. In future, we are concentrating to develop a new intrusion detection system that can be used to classify the normal and malicious activities in the network.

VI. **REFERENCES**

[1] Sunil Kim *, Jun-yongLee,“A system architecture for high-speed deep packet inspection in signature-based network intrusion prevention” ,Journal of Systems Architecture 53 (2007) 310–320.

[2] Vijayasarathy R, “A System Approach to Network Modeling for DDoS Detection using a Naive Bayesian Classifier”, 978-1-4244-8953-4/11/c (2011)@ IEEE.

[3] S. M. Fitaci, K. Jaffres-Runser and C. Comaniciu,” On modeling energy security trade-offs for distributed monitoring in wireless ad hoc networks,” Proc. Military Communications Conference, 2008. MILCOM 2008. IEEE, vol., no., pp.1-7, 16-19 Nov. 2008.

[4] N. Tsikoudis, A. Papadogiannakis and E. P. Markatos, ”LEoNIDS: a Low-latency and Energy-efficient Network-level Intrusion Detection System,” IEEE Transactions on Emerging Topics in Computing, Vol. PP, no. 99, 2014.

[5] Marti, Sergio, Thomas J. Giuli, Kevin Lai, and Mary Baker. "Mitigating routing misbehavior in mobile ad hoc networks." In Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 255-265. ACM, 2000.

[6] Liu, Kejun, Jing Deng, Pramod K. Varshney, and KashyapBalakrishnan. "An acknowledgment-based approach for the detection of routing misbehavior in MANETs." Mobile Computing, IEEE Transactions on 6, no. 5 (2007): 536-550.

[7] Sheltami, Tarek, Anas Al-Roubaiey, ElhadiShakshuki, and Ashraf Mahmoud. "Video transmission enhancement in presence of misbehaving nodes in MANETs." Multimedia systems 15, no. 5 (2009): 273- 282.

[8] E. M. Shakshuki , N. Kang and T. R. Sheltami "EAACK—A secure intrusion detection system for MANETs", IEEE Trans. Ind. Electron., vol. 60, no. 3, pp.1089 -1098 2013.

[9] D. Dong, X. Liao, Y. Liu, C. Shen and X. Wang, ”Edge Self-Monitoring for Wireless Sensor Networks,” IEEE Transactions on Parallel and Distributed Systems,” vol. 22, no. 3, March 2011, pp. 514-527.