International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 4 Issue 7, July-2015

# Analysis of SEAHN demand distance vector in Wireless mobile Ad-hoc Network

Sandeep Kumar[1], Col. (Dr) Suresh Kumar[2], Dr. Deepak Chhabra[3]

[1,2,3]Department of Electronics and Communication, U.I.E.T, MDU, Rohtak, Haryana, India

**Abstract: The growth of Mobile Ad hoc Networks (MANETs) has inflamed in current years mostly due to their benefits and their comprehensive applications. Mobile Ad-hoc Network is active peer-to-peer systems that contain of a group of Mobile nodes. These nodes perform multi-hop sensible transmission without needful a predefined organization. Recently, T-AODV & SEAHN plays a major role in the security of MANETs. Moreover, FIVE parameter availability, confidentiality, integrity, authenticity and Scalability are an effective way to detect various types of attacks in networks thereby securing the MANETs In this Thesis, we propose a new T-AODV (Ad Hoc trust based distance vector)&SEAHN(Stable Election Ad hoc Network)specially designed for MANETs. The proposed system introduces a new Ad hoc Trust and stable election routing protocol to inhibit the attacker from copying response the packets. Moreover, we suggest a trust prediction model to secure the network effectively and network lifecycle. The model can evaluate the trustworthiness of nodes, based on the generic behaviors of nodes. Finally, a multi-path secured routing scheme is used in this work. In this thesis we work on the PDR, Throughput and end to end delay.**

**Keywords: MANET, T-AODV, SEDV, Trust factor, Stable election, Mat lab.**

## I- INTRODUCTION

Mobile Ad-hoc Network (MANET) it is an independent group of Mobile operators that interconnect ended comparatively bandwidth forced wireless associations. In MANET one of the maximum themes in such networks is concert- in a dynamically varying topology; the nodes are predictable to be power-aware due to the bandwidth controlled network. Alternative problem in such networks is safety or security which is main concern in MANET security-subsequently each node donates in the process of the network correspondingly, the spiteful or malicious nodes are stimulating to detect. Here numerous submissions of Mobile ad hoc networks such as tragedy recovery processes, battle field transportations, etc. Toward study of these subjects, a situation based imitation inspection of a protected the routing protocol is done and is related with outmoded non-secure routing protocols. The developments used for the experiments signify critical real-world proposals such as battleground and saving processes, which incline to have challenging requirements. An exploration of the compromises between performance and security is done to improvement an understanding into the applicability of the routing protocols below consideration.

The Mobile Ad hoc networks or MANETs are the assembly of wireless networks which do not need any secure setup or base stations. They can be naturally prepared in places where it is demanding to process any wired organization. Such as presented in Fig.1, there are no base stations and each node necessity co-operate in advancing packets in the system.

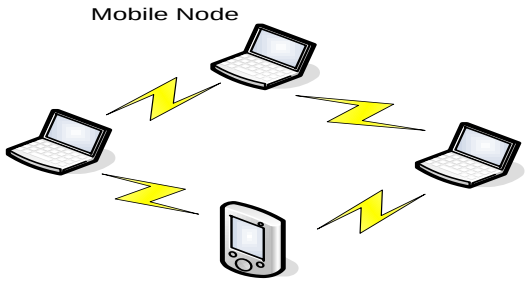


**Figure 1. A Mobile ad hoc network**

In this work, each node performances as a router which creates routing complex when compared to Wireless LANs, where the leading entrance fact acts as the router between the nodes[1]. A sensor network is an unusual group of Mobile ad hoc in wireless networks which contains of some sensors prepared without any secure organization. The change between sensor networks and standard ad hoc wireless is that the sensor nodes cannot be fundamentally Mobile. Advance, the sum of nodes is greatly developed than in normal ad hoc networks[2]. The nodes must have to more severe control stores then their purpose in exacting conservational circumstances. An instance of a sensor network is a normal of nodes checking the temperature of boilers in a current plant. And another application domain includes military, homeland security and medical care[4].

## II- METHODS

### 2.1 AODV (Ad-Hoc on-Demand Distance Vector Protocol)[8]

In this part we proposed the AODV routing protocol as quantified in the formof two Internet draft [Perkins and Royer 1998]. Pseudo-code for the protocol is given below. In AODV, a route to a purpose discovers the subsequentarenas[8]
Step 1: nextd: Subsequent node on a track to d.
Step 2: hopsd: distance from d, relaxed in the number of nodes (hops) that condition to be traversed to reach d.
Step 3: seqnod: Previous logged order number for d.
Step 3: life timed: The Outstanding time earlier route finish
The determination in order numbers is to pathway changes in topology. Every node saves its individual sequence number. It is incremented when the usual of residents of the node changes. When a route is documented, it is imprinted with the current order number of its endpoint. As the topology variations, more recent routes will have greater preparation numbers. That way, nodes can choose between new and outdated ways.
Once a node wants to intersect with an endpoint d, it broadcasts a route request (RREQ) message to all of its residents. The message has the following format:

**RREQ (hop to src; broadcast id; d; seqno; s; src seq no)**

Dispute hops to src controls the present coldness from the node that introduced the route request. The Original RREQ has this ground set to 0, and every following node increases it by one. The transmission id ground is a sole integer allocated to every RREQ originated by s. it is incremented afterward each RREQ. Dispute seqno class the smallest sequence number for a way to d that s is eager to receive (node s usages now the preceding sequence number it logged for the endpoint d, namely seqnod). Disagreement src sequence no is the seq number of the introducing node s. Once a node t accepts a RREQ, itrst forms whether it has a route to d obvious with a sequence number at least as immense as seqno. If it does not, it rebroadcasts the RREQ with incremented hops to src pitch. On the equal time, t can use the conventional RREQ to usual up an opposite route to s. This route would lastly be used to advancing answers back to s. If t has a renewed adequate route to d, it answers to s (advanced through the opposite route) with a route reply (RREP) communication which has the following format:

**RREP (hops d; seqnod; lifetimed):**

Advices hopsd; seqnod; and lifetimed are the consistent qualities of t's route to d. correspondingly, if t is the endpoint itself (t = d), it replies with

**RREP(0; d; large seq no; MY ROUTE TIMEOUT):**

The amount of large seq no needs to be at smallest as big as d's individual instruction number than and at smallest as immense as seqno since the application. Stricture MY ROUTE TIMEOUT is the defaulting lifetime, neighbouring organized at d. Each node that receives a RREP increases the value of the hops picketed and onwards the packed-to-end the opposite route to s.

Once a node obtains a RREP for certain purpose d, it usages info from the packet to explain its individual way for d. If it previously has a route to d, liking is decided to the route with a higher sequence number. If order statistics are the same, the smaller route is chosen.

This law is rummage-sale together by s and by all of the central advancing nodes. The preferred law is significant for dispersal error messages. In adding to the direction-finding table, all node s saves track of the active residents for both destination d.

**2.2 T-AODV (Ad-hoc Trust Distance Vector)[7][8]**

In Our proposed work overpowers the limits of the Trust-based source routing protocol and demonstrates to perform healthier than the existing system. We have comprised the adaptive trust close organization of the nodes by seeing both the individual trust values of every node and also the regular trust value of all the nodes in the trusted network. Adaptive Trust Level Classification delivers the required refuge by without humiliating the performance of the system and with no overheads to the system. By way of considering the average trust standards of the intermediate nodes to compute the route's trust

In this segment, a trust based system outline for fortifying Ad hoc On Demand Distance Vector Routing Protocol has been existing. In this device, Endless trust factor is used to appraise the trusted and straight path for statement in the network.
In the proposed scheme, a mechanism to check the next node whether it is trusted or not have been deployed where each node will be configured with the constant trust factor value, that value will be known to each and every node. The trust value is initiated in the route discovery phase. Each node keeps relentless trust values that will revolution in the RREP phase. Initially each node will be organized with the constant trust value 50 using node trust function. Source node broadcasts RREQ to adjoining nodes until an endpoint node having a route to destination determines, during this process hop count is prepared. If the present node is final terminus it will check trust value of previous hop and if it is not the destination then it will forward the request to all its neighbouring nodes. If the present node is last stop then it will evaluate the shortest path from destination to source.

AODV can first-class the better path (trusted and shortest) using trusts value and the amount of hops. When the RREQ and RREP message are made in the network, each node appends its own trust value to the trust accumulator on this route finding phase.
Each node also updates its own routing table. The subsequent method can be used to assess the right-hand and straight path.

**Sum of trust values * √No of hops/ No hops**
**Where, Sum of trust value = ∑ trust value**

**2.3 SEAHN**

The consequences designate that every trust-based routing protocol has its individual advantage. In specific, trust-based T-AODV routing upholds a steady throughput. Normal AODV, T-AODV , SEAHN with different node speed and different percentages of selfish nodes. It is Node would change route request RREQ when individual Node Energy threshold would be minimize from 0.5 jule. If Route Reply RREP receive from the crossover searching layer then link status will update the success route as in confidentiality and show remaining pending network Nodes. If normal Node ID is Include in crossover searching layer then advance node would cover for the normal node cluster which would be helpful for node stability. A network of 100 nodes with different percentages of selfish nodes, from 0% up to 30%, and moving at different speeds which would be improve average latency. Some points that can be observed . In the case that there are no selfish nodes in the mobile ad hoc network, both T-AODV and SEAHN have almost identical network throughput values.

**Assumptions:**

$S_d$ = Distance based node sequence
$F_{RREQ}$ = First Route Request
$NODE_{PRV}$ = Previous Node
Broadcasts RREQ packet:this protocol works in the route reply phase only .
If RREP packet received then
Sends data packets
Otherwise
$N_I$ ←Link Status for Next Hop Then RREQ=0; // where $N_I$ =Intermediate Nodes
End If
Verify Availability for trust Mechanism
while (prev)
{
if (Node_id->$N_t$)
{
prev = $N_{prev}$←$NA_{prev}$; // where $N_{prev}$ =previous Normal Node and
// $NA_{prev}$ = Previous of Advance Node

Advance node energy $S_n = S_d > D'$ (Sequence Node energy) ------significance of this equation…why we do need energy more than the destination node.

}
else {
k8
prev = $N_{prev}$← $NA_{prev}$;
if ((newnode->next = prev1->next))
newnode →next->prev 1
else
tail = newnode; prev->next = newnode; return; } }
If RREP packet received from suspected node then
Initiates a route to next node

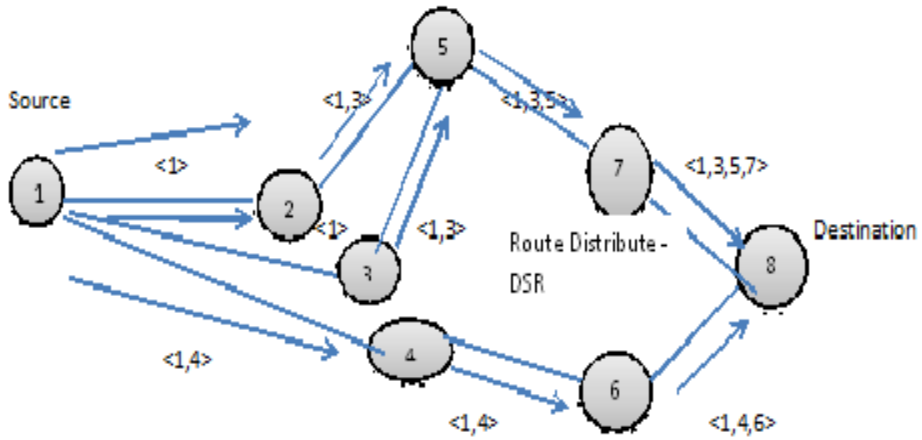


**Fig 2: T-AODV Route Discovery**

if( $T_{min}$ =no of node (node energy(in Jule)) ) //minmum Thrashold $T_{min}$
$S_{dst}$-- =>S, //Reverse route of source destination route should meet the trust
//requirement of the data packet. In other words, Non-Repudiated
// of the qualified route is greater than the requirement of the data
//packet. If such routes are found

nexthop=S,
hopcount=1
Sends FRREQ packet to next node
If FRREP packet received then
Extract FRREP packet information
If next node has a route to (destination &weak nodes) then
Discards FRREP packet
Unicasts RREP to source node
Otherwise Discards both RREP and FRREP packets
Broadcasts Normal energy node
while (prev)
{
if (then Node_id->N_sort < prev->Node_id->N_sort)
{
prev = prev->prev; // Go up the queue
}
else
{

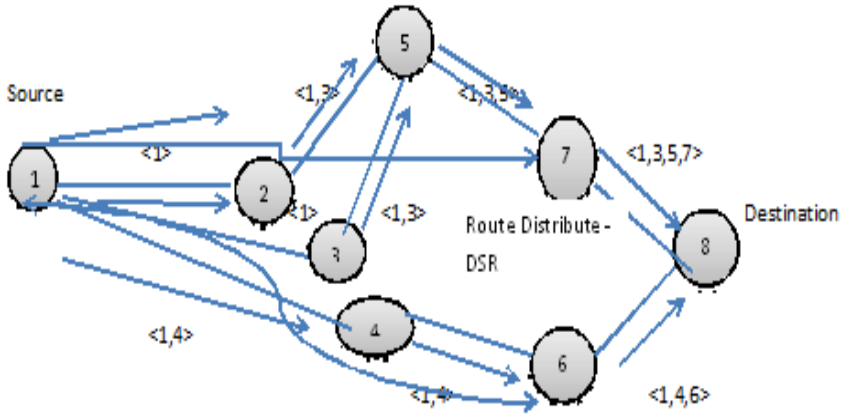


**Fig 3: SEAHN Route Discovery**

```
 newnode->prev=prev1;
if ((newnode->next = prev->next))
newnode->next->prev = newnode;
else
 tail = newnode;
 prev->next = newnode;
return;
}
 }
End If
End If
 End If
```

## III- Parameter Analyzed

Various parameters used for analysis are described below:
**Packet Delivery Ratio (PDR):** The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

**∑ Number of packet receive / ∑ Number of packet send**

**End-to-end Delay**:The average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

**∑ (arrive time – send time ) / ∑ Number of connections**

**Throughput:** The throughput of a receiver (per-receiver throughput) is defined as the ratio of the number of bits received over the time difference between the first and the last received packets.

## IV- RESULTS

The protocols are estimated for packet delivery ratio, throughput, path optimality and routing packet overhead. Throughput comparisons we know that throughput increases when connectivity is better.
It can be perceived that the performance of the AODV reduces drastically while T-AODV is slightly better among the three and SEAHN is better than T-AODV.
Throughput: It is well-defined as the total number of packets transported over the total simulation time.

The throughput assessment displays that the two algorithms performance margins are very close under traffic load of 50 and 100 nodes in MANET scenario and have large margins when number of nodes growths to 200. Mathematically, it can be defined as:

Throughput= N/1000 Where N is the number of bits established effectively by all destinations.

We applied our T-AODV and SEAHN algorithm in MATLAB and attained simulations. We assessed the presentation of T-AODV and SEAHN by measuring the number of broadcast aimed at 100 percent network attention of the MANET. Moreover, we restrained the performance time of the procedure for diverse network dimensions and different node we also assessed network coverage and implementation time of the algorithm for different localization achievement charges.
The performance of proposed T-AODV protocol is evaluated using imitation tool MATLAB and is compared with SEAHN routing protocol. The performance appraisal is done on the basis of following performance parameters:

1. Throughput
2. Packet Delivery Ratio
3. End to end delay

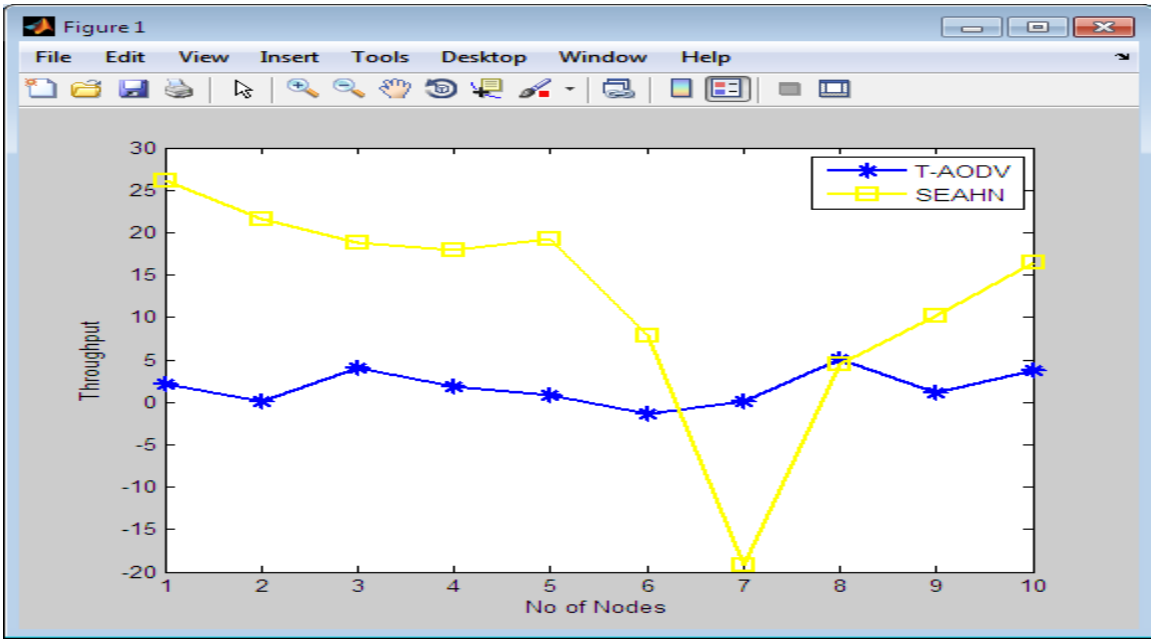


Fig 4: Improved attack Efficiency in Throughput

**Throughput time = Work-in-process/Throughput rate**

Throughput It is unique of the dimensional parameters of the network which provides the fraction of the channel volume used for useful broadcast chooses a terminus at the start of the simulation i.e., information whether or not data packets properly brought to the destinations. Throughput shown in the fig 4.

The capability to receive a packet during an impact can provide a number of significant assistances for wireless networking, with higher throughput, lower latency and improved spatial reuse. In this graph we show the Average latency of T-AODV&SEAHN over No. of Malicious node.

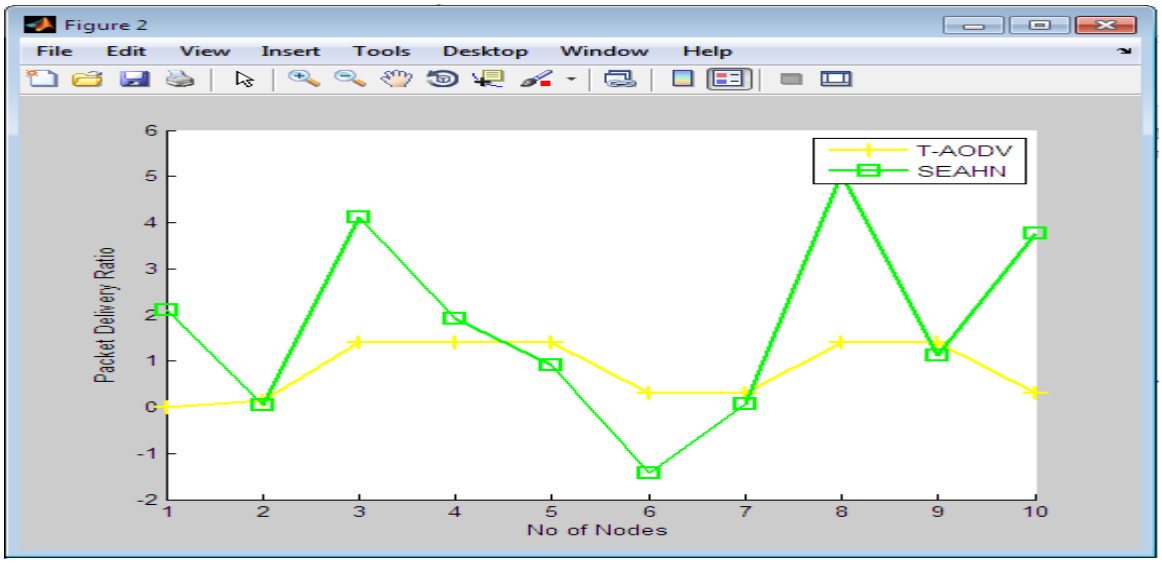


**Fig 5: Packet delivers Ratio of T-AODV & SEAHN**

PDR of T-AODV & SEAHN shown in the figure 5. Packet delivery ratio is distinct as the ratio of data packets established by the destinations to those produced by the sources. Mathematically, it can be defined as:

**PDR= S1÷ S2**

Where, S1 is the sum of data packets received by the every destination and S2 is the sum of data packets created by the every source. Graphs show the fraction of data packets that are successfully delivered during simulations time versus the number of nodes.

The normal rate at which is the entire number of statistics packet is transported positively from one node to add finished a communiqué network. Now, we must experimental that SEAHN has higher packet delivery ratio than T-AODV and AODV since of its table driven nature. This saves bandwidth and later increases performance.
But SEAHN performance fluctuates as the number of destinations increase. This is because after number of destinations increase with mobility T-AODV has to work harder to uphold the table. This signs to high load and hence performance squalor. T-AODV and SEAHN send packets all the time and waste bandwidth so their performance is summary. Accordingly, SEAHN performs better than T-AODV and AODV because of its proactive nature.

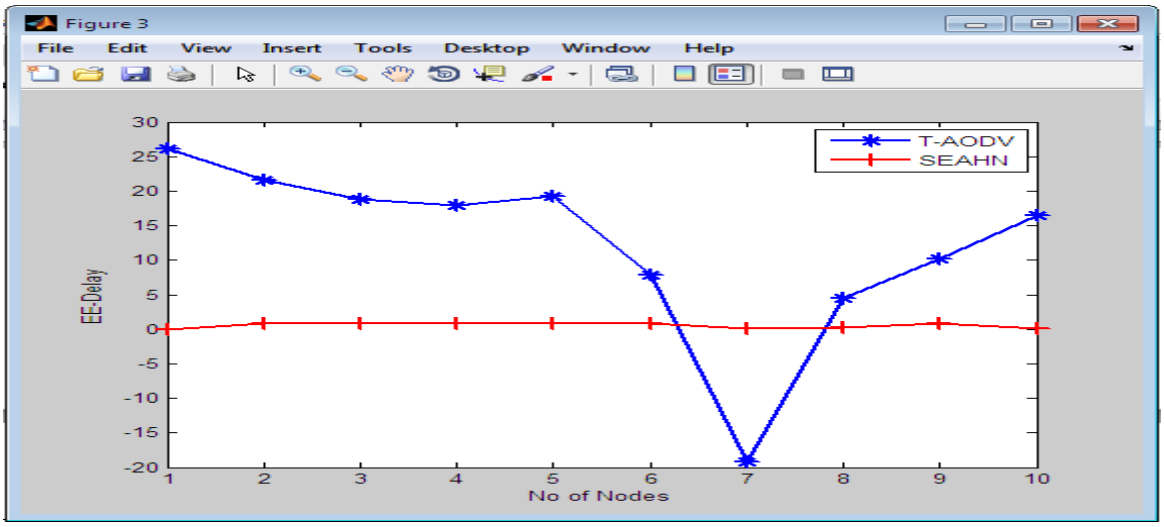


**Fig 6: end-to-end of T-AODV &SEAHN**

End to end delay is less of SEAHN as compare T-AODV. the average delay time of all successfully delivered packets. The average end-to-end delay of data packets is the interval between the data packet generation time and the time when the last bit arrives at the destination. As shown in Figure: 6, this simulation experiment showed us that T-AODV, SEAHN protocols are having higher end to end delays than others, indicating that the speed of simulation in large scale networks will be affected by this. This analysis exclusively deals with the network speed and communication effectiveness. Higher the delay, lower is the speed and possibility of packet drop and so needs the fault tolerance approach of selecting these protocols.

## V- CONCLUSIONS & FUTURE WORK

In this paper absorbed on the network PDR, Throughput and end to end delay it would be important to reflect other metrics like power consumption, the number of hops to route the packet, fault tolerance, minimizing the number of control packets etc., As above in figure 6 the path gaining optimal higher for SEAHN for initial stage of node discovery since it cover different path at the time of RREP but number of HOPs is same and elapsed time still minimized. The work can be extended by nitty-gritty study of routing protocols in a fault tolerant approach with proper simulation set up with parallel real time environment for mobile and wireless ad hoc networks.

This paper deals with the problem of unstable route for MANETs and presents a new route-stable routing protocol SEAHN. Adding the route stability arena to the RREQ packet in routing protocol avoids selection of unstable routes automatically during establishing a route. A make before break concept is proposed in the route repair mechanism of SEAHN. In the proposed routing protocol a new route is found, as far as possible, before a route break occurs instead of initiating a new source routing discovery as is done in AODV routing protocol. These provisions lead to an improvement in AODV routing protocol. The study is based on several simulation runs considering different performance evaluation metrics with varying pause times. We examined the enactment of T-AODV and SEAHN routing protocols on the basis of these metrics which include packet delivery fraction, end-to-end delay, normalized routing load, throughput and route life time with some security parameter which is authenticity, integrity, availability etc. The simulation runs better results for minimize drop packet on the basis of higher energy route and collect maximum packet delivered ratio , then control drop packet with lower energy nodes in distance vector in favor of SEAHN protocol . This is due to the proposed provisions which not only decrease the packet damage rate and the end-to-end delay but also improve the operation of the network resources increasing the throughput and average route lifetime.

**Future Work:**

In the future work of this Thesis can be complete in subsequent areas though, this research could be protracted to numerous stimulating educations as below.

1. Ways the identical study on other operating system surroundings
2. Conduct the same study on a wireless network
3. Conduct the same study on hardware routers

As there are vast variations on the VPN research area, there is a need for further research on the evaluation of the performance of many parameters involved in the VPN environment. This work will be extended to include a greater range of operating systems, protocols and metrics.

The show examination of alternatives of TCP below new routing protocols like DSDV, DSR, OLSR, GPSR etc. Cumulative the variety of result by seeing other new TCP_s like TCP/IP, TCP WESTWOOD for lower packet route.

## REFERENCES

[1]. Khelifa S., Maaza Z.M., “An Energy Multi-pathAODV Routing Protocol in Ad Hoc Mobile Networks” IEEE International Symposium on Communications and Mobile Network , 2010 Conference Publications, pp.1-4, 2010.
[2]. Maurya1 P.K., Sharma G., Sahu V., Roberts A. and Srivastava M., “An overview of AODV Routing Protocol” International Journal of Modern Engineering Research (IJMER), Vol.2, Issue3, pp.728-732, 2012.
[3]. Das S.R., Perkins C.E., Royer E.M., “Performance Comparison of Two on-demand Routing Protocols for Ad-Hoc Networks”, 19th annual joint conference of the IEEE Computer and communication Societies, IEEE Procc., pp.3-12, Vol.-1, Isreal, INFOCOM, 2000.
[4]. Thanthry N, Kaki S. R., Pendse R., “EM-AODV: metric based enhancement to aodv routing protocol”, IEEE 64th Vehicular Technology Conference, pp.1-5, 2006.

[5]. Yang H. , Li Z., "A Stability Routing Protocols base on Reverse AODV", IEEE International Conference on Computer Science and Network Technology, Vol.4, pp.2419-2423, 2011.
[6]. Li L., Chigan C., "Token Routing: A Power Efficient Method for Securing AODV Routing Protocol", IEEE International Conference on Networking, Sensing and Control, pp.29-34, 2006.
[7]. Yang H., Li Z., "Simulation and Analysis of aModified AODV Routing Protocols", IEEE International Conference on Computer Science and Network Technology, Vol.3, pp.1440-1444, 2011.
[8]. X. Li Z. Jia P. Zhang R. Zhang H. Wang "Trust-based on-demand multipath routing in mobile ad hoc networks" Published in IET Information Security School of Computer Science and Technology, vol-4, 2010.