

# The Energy Efficient Routing and High Security Transmission in Mobile Ad-hoc Networks

<sup>1</sup>G V Eswara Rao, <sup>2</sup>K V Chandra Sekhar

<sup>1</sup>Dept. of CSE, ANITS, Bheemunipatnam (Mandal), Vishakapatnam, Andhra Pradesh, India

<sup>2</sup>Dept. of Computer Science and Engineering, AITAM, Tekkali, Srikakulam, AP, India

## Abstract

In this paper we exhibit an overview of secure ad hoc routing conventions for mobile wireless networks. A mobile ad hoc network is a gathering of nodes that is associated through a wireless medium shaping quickly evolving topologies. The generally acknowledged existing routing conventions intended to suit the requirements of such self-sorted out networks don't address conceivable dangers going for the interruption of the convention itself. The suspicion of a trusted situation isn't one that can be sensibly expected; consequently a few endeavors have been made towards the plan of a safe and powerful routing convention for ad hoc networks. We quickly introduce the most prevalent conventions that take after the table-driven and the source-started on-request approaches. In view of this discourse we at that point define the risk demonstrate for ad hoc routing and display a few particular assaults that can focus on the activity of a convention. With a specific end goal to dissect the proposed secure ad hoc routing conventions structurally we have arranged them into classifications; arrangements in view of cryptography, arrangements in light of symmetric cryptography, notoriety based arrangements and a class of add-on components that fulfill particular security prerequisites. An examination between these arrangements can give the premise to future research in this rapidly developing region.

## Keywords

Manets, Access Control, Verification, and Transmission System Security, Data Transmission, Secured Routing

## I. Introduction

Mobile Ad-hoc Networks (MANETS) might be characterized as networks that have numerous free and self made nodes, here and there made out of mobile gadgets or other mobile pieces interconnected to each other by multi-jump wireless ways in an entirely distributed manner. Storing is an imperative piece of on-request routing convention for wireless ad hoc networks. The nodes participate to powerfully build up and keep up routing in the network. Correspondence is completed by sending bundles not specifically but rather inside the wireless range. Instead of utilizing the occasional or foundation trade of routing data regular in most routing conventions, an on-request routing conventions looks for the endeavors to find a course to some destination node just when a sending node starts an information bundle addressed to the node. An on request routing convention must store courses already found to keep away from the requirement for such a course revelation to be performed before every datum is sent. Numerous routing conventions for wireless ad hoc networks have utilized on-request instruments. A portion of those are Transiently Requested Routing Calculation (TORA), Dynamic Source Routing conventions (DSR), Ad-hoc on request separate vector (AODV), Zone routing convention (ZRP), and Location-Aided Routing (LAR). For example, in the Dynamic Source Routing convention, when some node

X starts an information bundle bound for a node Y to which S does not right now know a course, X starts another course revelation by starting a surge a demand comes to either Y or another node that has a stored course to Y, this node at that point comes back to X the course found by this demand. It might make an extensive number of demand parcels be transmitted, and add inactivity to the ensuing conveyance of information bundle that started it, henceforth performing such a course revelation can be an expensive activity. Be that as it may, this course disclosure can likewise be helpful as it might bring about the gathering of a lot of data about the present condition of network that might be valuable in future routing choices. Specifically, X may get various course answers in answer to its course revelation surge, every one of which returns data about a course to Y through an alternate segment of the network. The execution of this convention degrades quickly in high-versatility condition in light of the fact that the course upkeep component does not locally repair a broken connection. In this paper, for proficient looking, we have proposed a nonspecific seeking calculation on acquainted reserve memory association to speedier looking single/numerous ways for destination if exist in transitional mobile node store with a multifaceted nature  $O(n)$  (Where  $n$  is number of bits required to speak to the sought field). The other real issue of DSR is that the course support system does not locally repair a broken connection and Stale reserve data could likewise bring about irregularities amid the course disclosure/recreation stage. So to bargain this, we have proposed an enhanced store intelligence taking care of plan for on - request routing convention (DSR).

## II. Related Work

3.04 Tina Suen et al. [8] in 2005 They focused on recognizable proof and confirmation in ad hoc networks. Recognizable proof and validation are especially vulnerable to personality assaults, for instance, masquerading. For relieving the character assaults, they proposed to connect the message transmitter with an area and utilize this area data to discover personality. As indicated by the proposed technique, a Verifying Node (VN) confirms a transmitting peer node's area utilizing a mix of flag properties, trusted-peer coordinated effort, and worldwide situating frameworks (GPS) for recognizable proof purposes. In spite of the fact that they underscored toward the path data about companion character from flag's beginning, flag bearing without anyone else isn't a solid personality marker. In addition, they consider distinguishing proof in light of triangular situating framework where the three key focuses are The VN, confided in associate, and transmitter. At that point, triangulation and trigonometric capacities are utilized to compute the transmitter's area. Be that as it may, an issue happens when the three focuses lied on a same straight line. Additionally, computation in light of relative position isn't a proficient approach for recognizing a misleading node. 3.05 Shichun Pang et al. [9] in 2006 They presented an upgraded

vector space irrefutable SSS. The security of their proposed show depends on Elliptic Curve Cryptography (ECC) [10]. The model had precondition of  $(t, n)$  edge SSS. An evident framework gave in this paper recognizes the tricks from trustee and merchant. The common key dispersed by merchant is scrambled in light of ECC. It is guaranteed that the correspondence and calculation cost for their proposed mode is not as much as any current SSS. The key of elliptic bend cryptography has the length which is substantially less than RSA cryptography. In this manner, the model ought to be so vital in applications with restricted figuring force and memory. 3.06 Clare McGrath et al. [11] in 2006 They proposed distinctive key administration methods. For effective key administration for MANET, they distinguished numerous difficulties and research choices in their paper. It was recommended here that the unbalanced key encryption is more secure and adaptable than symmetric key encryption. At long last, accentuated to utilize such a PKI convention, to the point that may help calculation, correspondence, memory utilized and control limitations of MANET. 3.07 Wei Liu et al. [12] in 2006 They attracted thoughtfulness regarding ID-based Key Management (IKM) cryptography. IKM as an endorsement less arrangement helps open keys of mobile nodes to be specifically resultant utilizing their known IDs and some normal data. Thus, it expels the need of endorsement based verified open key dissemination, which is basic in traditional open key administration plans. Despite the fact that the analysts asserted in view of their reproduction result that, IKM is more effective and improved when contrasted with ordinary endorsement based approval; however with no single declaration key age specialist like Kerberos, the one of a kind age of ID for a disseminated framework is hard. 3.01 Donald Welch et al. [3] in 2003 The creators overviewed over different wireless security dangers and their counter measures cryptographic strategies. They ordered the dangers in view of various security issues. Movement investigation, detached spying, and dynamic listening in are three ordered assaults that abuse classification or protection of the session. The man-in-the-center assault opposes both privacy and honesty. The rest three assaults, specifically unapproved get to, session seizing and the replay assault break the respectability of the network movement. For the counter measures, the scientists proposed to locate an incorporated secure system having reasonable confirmation instrument alongside a solid and secure encryption calculation utilizing piece figure. 3.02 Ravi K. Balachandran et al. [4] in 2005 They proposed a productive key understanding plan in particular Chinese Remainder Theorem and Diffie-Hellman (CRTDH). As per this CRTDH, there is no pre-shared mystery between the individuals and the administration of a trusted specialist or a gathering controller isn't required. CRTDH utilizes the Diffie-Hellman key trade and the Chinese Remainder Theorem for proficient key assentment of Symmetric Cipher. Part serialization and focal specialist are two noteworthy issues of SGC conspire which are explained by CRTDH. Uniform workload appropriation for every one of the individuals, productive calculation of gathering key and few rounds of re-keying are more highlighted by this convention. Be that as it may, CRTDH experiences man-in-the-center assault; likewise it isn't streamlined for a versatile ad hoc network. The CRTDH depends more on the confirmation of SSS to end up effective [5].

### III. The Routing Protocols in Mobile Ad-Hoc Networks (MANETS)

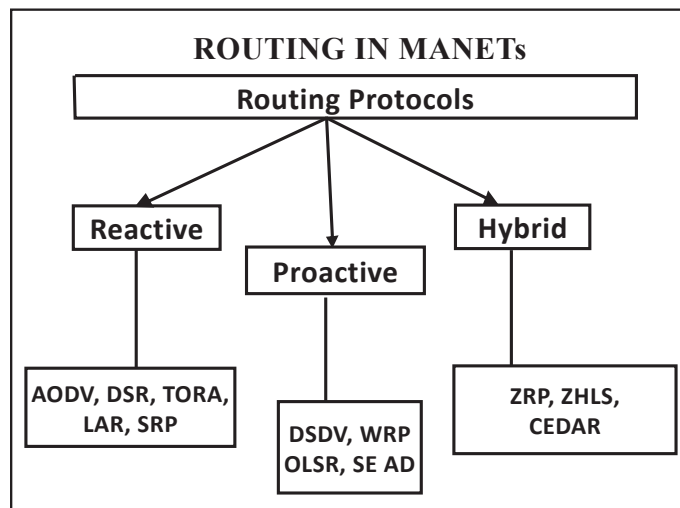


Fig. 1: Different Routing Protocols in MANETS

The fundamental objective of directing conventions in specially appointed systems is to figure out the ideal way with least overhead, least transfer speed utilization and least defer between the source and the destination node. As a large portion of the nodes in specially appointed systems are remote versatile nodes, the topology of such sort of a system does not stay altered. Thus, it turns into the node's obligation to consistently find the system topology with a specific end goal to course the messages appropriately. Hence, there is a requirement for different directing conventions to find an ideal way from the source to the destination. A solitary routing convention can't work ideally in distinctive system situations. A need is along these lines felt for a proper convention choice taking in thought diverse system parameters, for example, thickness, size and the versatility of the nodes [5]. On the premise of the system topology, the routing conventions in MANETS are comprehensively sorted as Proactive Routing Protocols, Reactive Routing Protocols and Hybrid Routing Protocols which are talked about as takes after:

#### A. Proactive Routing Protocols

In the proactive directing conventions, routing is done utilizing the data present as a part of routing tables kept up at every node i.e. table driven directing. These tables are traded on an occasional premise between the nodes. Every passage in the table contains the data of the following jump for coming to a node or subnet and the expense of this course. Since data of the neighboring nodes is kept up at every node, the ideal opportunity for course determination gets to be insignificant. Taking after are the issues from which genius dynamic routing calculations endure: a) Dynamic topology of the system results in some incessant changes in the directing table bringing about invalid courses as the new courses can't be upgraded every now and again. Accordingly, there is a moderate response on rebuilding and thus, the disappointments of connections. b) Increase in system size results in expansion in size of directing table which thus expands the system load while redesigning or trading tables. Situations for which these sorts of conventions are most appropriate are: i) Lesser node versatility ii) Lesser thickness or less nodes iii) Small measured systems. Different star dynamic routing calculations are Optimized Link State Routing (OLSR) [10], Landmark Routing Protocol (LANMAR) [11-12].

## B. Reactive Routing Protocols

If there should arise an occurrence of Reactive Routing conventions, the directing is finished by the nodes just on interest i.e. just when the node needs to communicate something specific. The sender surges its neighbors with Route Request (RREQ) packets to discover course in the system. Any destination/middle of the road node in the system having way to the destination will answer back with Route Reply (RREP) to the sender and the routing is refined. These experience the ill effects of taking after impediments: a) There is a period delay in discovering the courses following an extensive number of control bundles must be traded before the trading of genuine information. b) Network blockage may come about because of unreasonable flooding of bundles. Receptive Routing discover their applications in the accompanying system situations: i) High portability systems. ii) Medium size systems. Different Reactive routing calculations are Ad Hoc On-Demand Distance Vector (AODV)[13], Dynamic MANETS On Demand (DYMO)[14], Admission Control empowered On interest Routing (ACOR)[15].

## 3. Hybrid Routing Protocols

Crossover Routing Protocols exploits both responsive and genius dynamic directing calculations. In the introductory stages, the nodes recognize the courses utilizing some professional dynamic calculations and later on utilizations receptive calculations for on interest directing. Both professional dynamic and responsive nature of the convention can be utilized reciprocally relying upon the diverse system situations. Since neither unadulterated proactive nor the receptive methodology can alone handle all the system necessities, so the half breed methodology may be by and large the ideal decision. The primary weaknesses of such calculations are: i) Number of initiated nodes decides the favorable position that can be taken ii) Reaction to the activity interest relies on upon the angle of movement volume. Different Hybrid directing calculations are Zone Routing Protocol (ZRP) [17], Zone-Based Hierarchical Link State (ZHLS) [16].

## IV. Security Issues

The MANETS set new difficulties for system security and the need of an hour is to give careful consideration to the security dangers postured on the system. Taking after are the concerned issues in security of impromptu systems:

### A. Nodes Acting as Routers

As nodes themselves are taking an interest in transferring of messages, any malignant node in the system can without much of a stretch abuse the message activity either by generating so as to drop messages or false messages and so forth.

### B. Constrained Resources

Due to the constraint of system assets in portable impromptu systems, the different cryptographic arrangements relevant to wired systems are not straightforwardly pertinent. Along these lines there is a requirement for new security arrangements which can discover their application in this testing area.

### C. Versatility of Nodes

Dynamically changing system topology results in more open doors for the malevolent nodes to assault.

### D. Area of Nodes

Since Ad hoc systems are shaped for a reason, the arrangement

environment may not be exceptionally security touchy. For Example, the nodes sent in the front line or in the woodlands for following wild creatures and so on may welcome numerous security dangers and assaults.

## E. Remote Medium

Interoperability is simple in a remote medium. Consequently, there is an absence of protection and the critical messages can be listened stealthily and adjusted effectively.

Some fundamental security limitations that must be considered and actualized in Wireless specially appointed systems are:

### 1. Confidentiality

Confidentiality in the system must be executed to keep the exposure of any piece of the data to unapproved elements amid the transmission of information. Certain delicate utilizations of specially appointed systems may face wrecking results if classification is not dealt with.

### 2. Integrity

Integrity is damaged when a message is effectively changed in travel. The system ought to have the capacity to keep up the trustworthiness so that the unapproved substances are not ready to adjust/degenerate any message.

### 3. Availability

The principle reason for development of any system is to trade data. This system security requirement guarantees the information accessibility in the system. This limitation can be abused by the refusal of administration assaults (DoS) in the specially appointed systems.

### 4. Authenticity

Authenticity guarantees that a node is a real or trusted node in the system. Without confirmation any malignant node can cheat a bona fide node and along these lines can have an entrance to the secret data. Non-renouncement:

Non-revocation guarantees that no node can decline the activity that it has performed i.e. every node assume the liability of its activities. This property of the system permits the defective node discovery and henceforth helps in its detachment from the system. For e.g. at the point when a node X gets a message with its trustworthiness limitation abused from another node Y then X can announce Y as a vindict

## V. Proposed Methodology

To disclose the hidden pattern in communication system, our proposed system composed of two steps. First, it constructs point-to-point traffic matrices by using the raw captured packets and constructs end-to-end traffic matrix. Second, it identifies the source node and destination node with the possible probability. This working model is illustrated in Fig.2 in as system architecture that the function taken place. Initially we need to build the point-to-point matrices with the captured packets at the certain period T. Time slicing technique is used to avoid the point-to-point traffic matrix from containing two dependent packets which takes the snapshot of entire network. Fig.2. Working Model of STAR With a sequence of point-to-point traffic matrices we derive the end-to-end traffic matrix. This is termed as accumulative traffic matrix. We assume the timing and hop count thresholds with the end-to-end matrices which do not filter any packet in the network. The deduced end-to-end traffic matrices are still need to perform the

further implementation to identify the actual source and destination probability distribution and end-to-end link probability. Finally evaluation is done with the probability distribution vectors in which all the vectors are normalized and it make sense only to the relative orders among the elements of each vector. In this paper, we present different modules such as topology module, attacker’s module, etc.

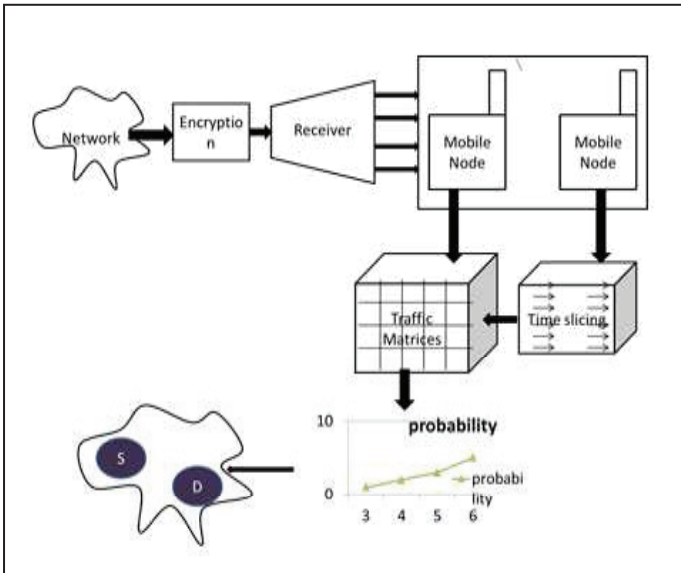


Fig. 2: Proposed System Architecture

**A. Proposed Algorithm**

- Step 1:** The data is sent from the source.
- Step 2:** The data is passed through the network provider which verifies the sent data.
- Step 3:** The data is divided into several small packets according to the size of the nearest node.
- Step 4:** The small packets of data are scanned and their performance is checked.
- Step 5:** If the size of the packet match the size of the node, it will be sent to the node.
- Step 6:** If the size of the packet do not match the size of the node, it will be again sent to the network provider for verifying.
- Step 7:** The matched packet of data is sent to the destination.
- Step 8:** The mobile server receives the data without any drop.
- Step 9:** The data is sent to the destination.

The formulation of intended Dynamic source routing algorithm in the proposed scheme with n nodes is presented as follows:

$$C = \frac{\sum_{i=1}^n X_i}{n} \tag{1}$$

Where  $X_i$  denotes location of nodes in the network. After specify centre nodes C, the average distance between C and all the nodes of network R is calculated as presented below:

$$R = \frac{\sum_{i=1}^n |X_i - C|}{n} \tag{2}$$

Then, the location of means  $m_i$  (m<sub>i</sub>· mix) in each cluster according to R and C values is computable.

In this scheme, the calculations of means are sorely important because the appropriate locations of opted means are cause of a fair nodes distribution in each cluster.

After determining the position of K-means, n nodes of network should properly distribute into K clusters. For this purpose, the presented equivocation is used:

$$avg_s \text{ mir. } \sum_{i=1}^k \sum_{x_j \in S_i} |x_j - m_i|^2 \tag{3}$$

Where,  $S_i$  denotes Clusters and is function of minimum average distance. In this method, each node is joined to closest cluster.

In order to creation clusters with a fair distribution, minimum average distance of nodes to each cluster has been estimated and each node exactly attach to one nearest cluster. Therefore, the final created clusters can be described as follows:

$$S_i^{(t)} = \{x_j | |x_j - m_i^{(t)}|^2 \leq |x_j - m_{i'}^{(t)}|^2\} \tag{4}$$

When all the nodes would be attached to clusters, the formation of all the clusters is finalized.

**Algorithm 1** Pseudocode of the best answerer identification executed by node  $i$ .

- 1: **Input:**  $ID_i, ID_j, Q_{(i,j)}$  ( $j \in \mathcal{F}_i$ )
- 2: **Output:** top- $K$  best answerers
- 3: //Periodically update  $Q_{(i,j)}$  ( $j \in \mathcal{F}_i$ )
- 4: **for** each friend  $j$  in friend list  $\mathcal{F}_i$  **do**
- 5:     Update  $Q_{(i,j)}$  based on Equation (2)
- 6: **end for**
- 7: **if** create a question or receive a question it cannot answer **then**
- 8:     **if** TTL>0 **then**
- 9:         **for** each friend  $j$  in friend list  $\mathcal{F}_i$  **do**
- 10:             Calculate  $S_{(q_i,j)}$  using  $ID_{q_i}$  and  $ID_j$  based on Equation (1)
- 11:             Calculate  $BA_{(i,j)}$  using  $Q_{(i,j)}$  and  $S_{(q_i,j)}$  based on Equation (3)
- 12:             Add  $BA_{(i,j)}$  to a list *List*
- 13:         **end for**
- 14:         QuickSort partition around the  $K^{th}$  largest element in *List*
- 15:         Find the top- $K$  friends having the highest  $BA_{(i,j)}$
- 16:         TTL=-1
- 17:         Send the question to the identified  $K$  friends
- 18:         **end if**
- 19:     **end if**
- 20: **if** does not receive answers for its created question during the time corresponding to TTL **then**
- 21:     Resort to the centralized server for the answers
- 22: **end if**

**VI. Simulation Results and Analysis**

In this paper, we will try to compare the results of two Routing Protocols, one is Proactive Protocol and another one is Reactive Routing Protocol. Reactive includes AODV (Ad-Hoc on Demand Distance Vector) Routing Protocol and Proactive includes DSDV (Destination Sequences Distance vector) Routing Protocol on the basis of Average End to End Delay, Network Load, Throughput and Packet Delivery Ratio (PDR) quantitative metrics using Riverbed Simulator. The AODV and DSDV Routing Protocols will work on TCP traffic pattern by creating the scenario with fixed number of nodes at constant 3600 sec simulation time. Transmission Control Protocol (TCP) is one of the core Protocols of the Internet Protocol suite referred to as TCP/IP. The simulation setup has been comprises 50 fixed nodes at a speed of 10 m/sec with heavy FTP traffic. The simulation has been performed in Office Network Environment with 1 x 1 kilometers squared space.

**A. RIVERBED Modeler**

There are a variety of software are widely available, such as NS2 [29-30], RIVERBED (OPNET) [31], OMNeT++, QualNet [32], GloMoSim to perform simulations of MANET Routing Protocols, in which we use RIVERBED Modeler version 17.5. Our reason for selecting RIVERBED is as a result of its key features; providing solutions for constructing networks and applications and it usually gives perfect results. Riverbed Modeler is formerly known as OPNET Modeller Suite. OPNET stands for Optimized Network Engineering Tools. The use of RIVERBED is broken down in four major steps- modeling (creating network nodes), then choose statistics, run simulations and finally view and analyze results. The Results of our Simulation are: Throughput:

Throughput is the number of packets that are passing through the channel in a particular unit of time and it can be improved with increasing node density. It is usually measured in byte/sec or bits/sec [3]. Some factors affects the Throughput as- if there are many topology changes in the network, unreliable communication between nodes, limited bandwidth available and limited energy. High Throughput is always expected for any Routing Protocol.

In fig. 4, we compare DSDV and AODV Routing Protocol with the help of Throughput factor. In this, it can be clearly seen that, DSDV Routing Protocol is showing higher Throughput than AODV Routing Protocol of the network of 50 fixed nodes for TCP traffic. In the time interval of 1200 to 3600 sec., maximum amount of packets have been delivered from source to destination node in terms of DSDV because it is a Proactive type Routing Protocols and advantage of these type of Protocols is there are no delay to find out the route from source to destination nodes because path is immediately available when source need to send a packet. For the same time interval AODV does not performs well because of less active route.

**B. End to End Delay**

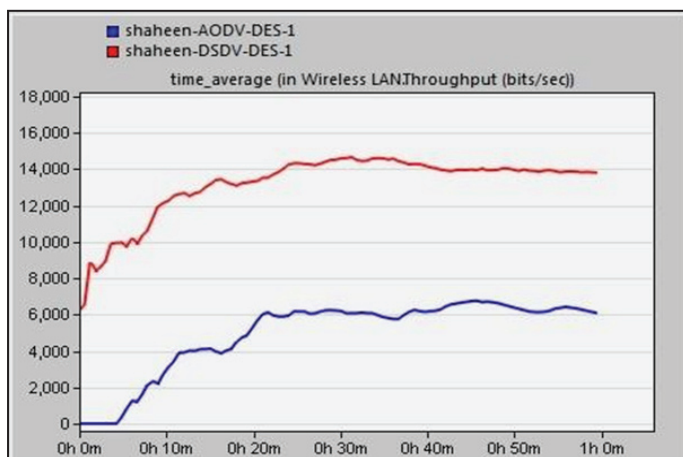


Fig. 4: Throughput

The packet End-to-End Delay (EED) is the average delay of data packets from source to destination. It is also called Data Latency. It is expressed in seconds [4]. EED includes route discovery, propagation, queuing, and transfer delays.

In fig. 5, plots are shown between AODV Routing Protocol in comparison with DSDV Routing Protocol for End to End Delay factor. The comparison is clearly showing that DSDV Routing Protocol is showing higher End-to-End Delay than AODV Routing Protocol with 50 fixed nodes setup in environment. The delay in DSDV is high because in that particular time interval the distance between sending node and receiving node is high due to traffic.

One reason for the degradation in the End-to-End Delay of DSDV is at higher number of nodes is attributed to its route discovery process. However, the performance of AODV improves with the increase in the number of sources. The reactive nature of AODV helps to reduce the End- to-End Delay.

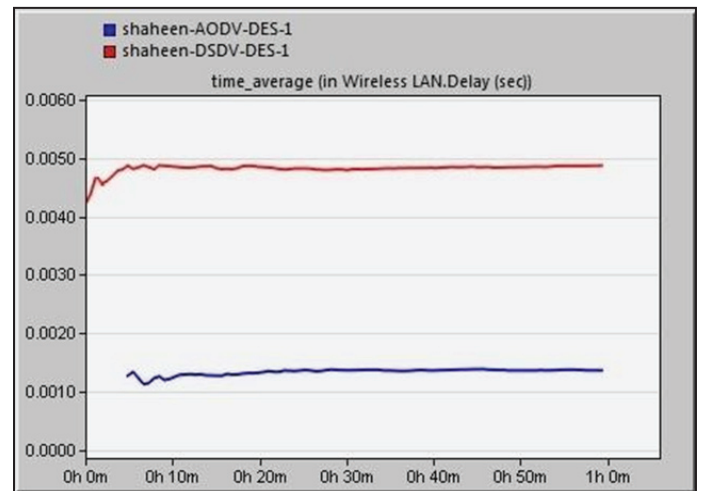


Fig. 5: End-to-End Delay

**C. Packet Delivery Ratio (PDR):**

Packet Delivery Ratio (PDR) is the ratio between the number of received packets by destination node and the number of data packets sent by source node. It characterizes both the correctness and efficiency of Ad- hoc Routing Protocols. A high Packet Delivery Ratio (PDR) is preferred in a network [35].

In fig. 6, Packet Delivery Ratio (PDR) is being shown between DSDV and AODV Routing Protocol, using 50 nodes for FTP application. The DSDV Routing Protocol outperforms AODV routing protocol in terms of PDR with average time interval. This is because, as number of nodes increases, PDR will also increase in DSDV Routing Protocol with respect to time, taking delay as less important factor. The major cause of low PDR is the use of TCP traffic. TCP suffers massive degradation because of rampant retransmissions.



Fig. 6: Packet Delivery Ratio

**D. Network Load**

It represents the total load measured in bits/sec, which is submitted to wireless LAN layers by all higher layers in all WLAN nodes of the network. It shows the effectiveness of Routing Protocols when the packets are being received. The larger this fraction is, the less efficient the Protocol is.

Proactive Protocols are expected to have a higher load than reactive ones. It can be seen in Figure 4 as expected; the Network Load in DSDV is higher than AODV. Although, the reactive nature of AODV Routing Protocol causes more number of control overhead than DSDV and normalized routing load for AODV is high. In spite of that, DSDV is Proactive in nature, maintains routing table regularly hence have large routes MAC overhead, which automatically increases overall Network Load.

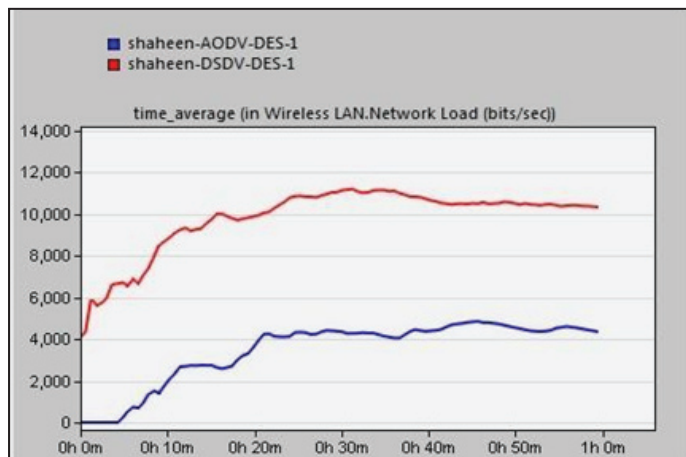


Fig. 7: Network Load

## VII. Conclusion and Future Work

A comparison of different techniques for energy efficient and secured routing is carried out. From the survival study, it is clear that MBMA-OLSR routing scheme was not appropriate for large-scale network and multi-hop networks. Energy-efficient secured routing protocol failed to recognize the external attacks with lesser energy consumption. The traffic load balancing settings were not accepted in secret-common-randomness establishment algorithm. SUPERMAN targets MANET attributes and it is not suitable for additional types of network. Throughput level was not improved using the SUPERMAN protocol. The wide range of experiments on existing techniques analyzes the comparative performance of various energy efficient and secured routing techniques and its drawbacks. Finally, from the result, the research work can be carried out to minimize the energy consumption and improve the security level in future. The proposed system will observe the traffic pattern of the adversary. As nodes are hidden in mobile networks a heuristic searching algorithm will be applied. Nodes. Probability of point to point transmission among receivers will be estimated by point-to-point traffic matrix. Then multihop traffic and performing probability distribution the traffic pattern will be discovered. This will provide an approximate traffic pattern with approximate source and destination in the network. The proposed system will reduce the issue of anonymous communication in mobile networks.

Future Scope: Furthermore, to analyze the traffic before sending the packets to the destination. For single destination which have many paths to reach from source. So in case of traffic, user can choose an alternate way to send a message to destination.

## References

- [1] Darren Hurley-Smith, Jodie Wetherall, Andrew Adekunle "SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad-hoc Networks", IEEE Transactions on Mobile Computing, pp. 1-15, 2016.
- [2] S. Zhao, R. Kent, A. Aggarwal, "A key management and secure routing integrated framework for mobile adhoc networks",

Ad Hoc Networks, Vol. 11, No. 3, pp. 1046-1061, 2013.

- [3] A. R. McGee, U. Chandrashekar, S. H. Richman, "Using ITU-Tx. 805 for Comprehensive Network Security Assessment and Planning", pp. 273-278, 2004.
- [4] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "Security in Mobile Ad-hoc Networks: Challenges and Solutions", Wireless Communications, IEEE, Vol. 11, No. 1, pp. 38-47, 2004.
- [5] D. Smith, J. Wetherall, S. Woodhead, A. Adekunle, "A Cluster-based Approach to Consensus based Distributed Task Allocation", In Parallel, Distributed and Network-Based Processing (PDP), 2014 22<sup>nd</sup> Euromicro International Conference on. IEEE, 2014, pp. 428-431.
- [6] Revathi Venkataraman, M. Pushpalatha, T. Rama Rao, "Performance Analysis of Flooding Attack Prevention Algorithm in MANETs", World Academy of Science, Engineering and Technology 2009.
- [7] M.A. Shurman, S.M. Yoo, S. Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, pp. 96-97, 2004.
- [8] J. CAI, P. YI, J. CHEN, Z. WANG, N. LIU, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network", 2010 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), Perth, Australia, pp. 775-780, 2010.
- [9] T.H. Clausen, G. Hansen, L. Christensen, G. Behrmann, "The Optimized Link State Routing Protocol, Evaluation Through Experiments and Simulation", Proceedings of IEEE Symposium on Wireless Personal Mobile Communications 2001.
- [10] M. Gerla, X. Hong, L. Ma, G. Pei, "Landmark Routing Protocol (LANMAR) for Large Scale Ad Hoc Networks", IETF Internet Draft, Vol. 5, 2002.



G V Eswara Rao, received his B.Tech, M.Tech from Narasaraopeta Engineering College, Andhra Pradesh, India. Present, he is working as Assistant Professor in the CSE Department of Anil Neerukonda Institute of Technology and Sciences Bheemunipatnam (Mandal) Vishakapatnam, A.P., India. He participated in various workshops, seminars and presented papers related to advanced technologies. His areas of interests includes Computer Networks,

Compilers, Automata Theory, and BigData.



Kattamuri Venkata Chandra Sekhar received his B.Tech in Computer Science Engineering from Sri Sivani College of engineering the University of Jntu Kakinada and M.Tech (CSE) department of computer science engineering from AITAM, Tekkali, Srikakulam, AP, India. Present he is working as Assistant Professor in the CSE Department of AITAM, Tekkali, Srikakulam, AP, India. His areas of interests includes Computer Networks,

Data Mining.