# Effective Routing Protocol And Analysing Various Attacks In The Manet Network

**M V S SNagendranath, A. Ramesh Babu**

***Abstract*: Mobile Ad-hoc Network is the self-configuring structure less network for transmitting the information from one node to another node because of the independent node direction. During the information transmission in the network one of the main challenges is to maintain the intermediate node information for making the effective transmission. In addition the intermediate person may be hacking the information by performing the Wormhole and Black hole attacks. So, in this paper proposes an effective Neighboring Relationship based Clustering protocol. The protocol analyzes the neighboring relationship between the transmitted node information protocols. Each similar node information is grouped into the cluster. At the time cluster head and neighboring node topology has been updated continuously for avoiding the middle man attacks like, wormhole and black hole. Further the energy consumption is managed by applying the Fireflies algorithm based Energy efficient routing protocol with efficient manner. Then the efficiency of the system is analyzed using the experimental results like, packet delivery ratio, energy utilization factor and percentage of attack free routing efficiency.***

***Keywords* : Black hole, Fireflies algorithm based Energy efficient routing protocol ,Mobile Ad-hoc networks, Neighboring Relationship based Clustering protocol.***

## I. INTRODUCTION

Mobile Ad hoc Network (MANET) is one of the most self-configuring and infrastructure less network that helps to transmit the information from source to destination. During the information transmission process the network utilize the different characteristics like light weight topology, multi hop routing, distributed operation, confidentiality, availability and integrity [1]. Even though the MANET consists of various characteristics it has some of the challenges like limited bandwidth, battery constraints, hidden terminal problem, mobility induced route change, transmission error, scalability and cooperativeness. These challenges are leads to create the intermediate attacks reply attacks, snooping, passive attacks, active attacks, denial of service attack, black hole attack [2]. These attacks are access the MANET network structure and the change the information which leads to affects because the MANET based information transmission used in various applications like, bank transaction, medical systems and so on. From the above discussed attacks the MANET needs the high security approaches and techniques to avoid the drawbacks present in the mobile ad hoc system [3]. The flexibility of the networks helps to transmit the information with high degree but the attacks and intermediate access need to be corrected by applying the various wireless and cryptographic techniques.

So, various researches introduce the cryptographic techniques to analyze the information and user details before and after sending the information in the network. The security method distributes the node in the different location and particular secret key has to be maintained to verify the information in the network. By using the above concept different protocols like Ad hoc On-demand Distance Vector, Dynamic Source Routing Protocol, and Zone Routing Protocol are used to establish the route between the source and destination with effective manner [4]. At the time of routing process, different energy consumption, power saving, attack free method is used to ensure the secure transmission of the particular information. Even though the researches utilize the effective routing protocol still it has some of the issues like packet delivery ratio, bandwidth usage and percentage of routing efficiency [5]. These issues are further create the wormhole and black hole attacks in which the worm hole attack is one of the dangerous attack in which the data's are recorded continuously by placing the two attackers in the network.

Then the issues present in the network protocols are overcome by applying the novel clustering and optimized techniques based routing protocol. The method analyzing the nodes present in network using the neighboring relationship concept and the similar nodes are grouped together formed as the cluster. The formed cluster head has been continuously updated to eliminate the attackers activities because the attackers are difficult to estimate the flow of data also the content of the data. During the transmission, the energy consumption is done by applying the Fireflies algorithm based Energy efficient routing protocol. The efficiency of the system is evaluated with the help of the experimental results and discussions. The rest of the paper is organized as follows. Section 2 describes about the related works on the routing protocol and the related attacks. Section 3 analyze the proposed system methodologies, section 4 discusses the effectiveness of the proposed system. Section 5 concludes the proposed work.

**Revised Manuscript Received on August 13, 2019.**

**M V S S Nagendranth***, Research Scholar,( Correspondence Author)
Department of Computer Science and Engineering ,Hindustan Institute of Technology and Science, Rajiv Gandhi Salai, Old Mahabalipuram Road, Padur, Kelambakam, Chennai, Tamil Nadu 603103. Email: nagendranath@sasi.ac.in

**Dr A. Ramesh Babu**, Professor & Head Department of Science and Humanities, Hindustan Institute of Technology and Science, Rajiv Gandhi Salai, Old Mahabalipuram Road, Padur, Kelambakam, Chennai, Tamil Nadu 603103. Email: arbbabu67@gmail.com

## II. RELATED WORKS

In this section discusses about the various routing protocol for handling the various intermediate attacks present in the mobile ad hoc network. Tarek et al., [6] implementing the security based mobile ad hoc networks communication system. During the information transmission, black hole attack is one of the most important attacks which track all the data. So, author utilizes the ad hoc on demand distance vector protocol with intrusion avoidance system to eliminate the intermediate access of the information. This system is implemented in the NS2 simulator tools and the efficiency of system is evaluated in terms of the normalized routing load, packet delivery ratio and throughput which are compared to traditional ad hoc demand distance vector. Sonal et al., 2015 [7] investigating the sinkhole attacks present in the wireless network using the dynamic source routing protocol. The method efficiently analyze the source and destination by passing the two important messages like RREQ – Route Request and RREP – Route Reply for routediscovery process. According to the routing protocol the intermediate attacks are successfully eliminated. Then the efficiency of the system is implemented with the help of the NS2 tool in which the network does not have any intermediate attacks. Further the proposed system reduces the sinkhole attacks upto 32% when compared to the existing methods.

Mohammad Al-Shurman et al., [8] developing the efficient communication system by reducing the black hole attacks in the MANET communication network. The author analyzing the solutions in two ways, initially the effective source and destination need to be selected using the ad-hoc networks. After estimating the affective route and the packet sequence and packet header need to be selected with effective manner. The implemented system is compare with the existing and traditional system and the author introduced system is verified from 75% to 98% which ensures the optimal and secure route with minimum delay and cost. Chaitas Shah et al., [9] developing the secure mobile ad hoc network by eliminating the black hole attack using the zone routing protocol. The author implemented zone routing protocol has the advantage of both proactive and reactive methods which successfully eliminates the intermediate attacks. The method forms the zone that ability to transmit the packets also eliminates the vulnerabilities present in the network. During the transmission the packets are integrity with the network to avoiding the black hole attack. Then the efficiency of the system is analyzed using the experimental results and discussions in terms of the packet delivery ratio with the packet loss problems.

Dharman, et a., [10] avoiding the grey hole attack present in the network by utilizing the secure message digit method with the adhoc networks. The method analyze the network structure in the various direction also estimate the source and destination node in the network. The grey hole attack involved in the network and drop the packet by performing the intermediate operation. So, the source and destination is identified and encrypt with the message digit technique which is difficult to guess the actual communication path. From the estimated path an ad hoc routing protocol transmit the information with effective manner. Then the efficiency of the system is analyzed in terms of the packet delivery ratio which is implemented with the NS2 simulation tool. PrachiGoyal et al., [11] implementing the effective and secure mobile ad hoc network system by eliminating the various attacks like denial of services, alteration, fabrication attacks and black hole attack. Among the various attack, the black hole attack is one of the most severe attack which hack the data during the communication. So, these attacks are eliminated by effective reactive and proactive routing protocols. The efficiency of the system is implemented with the help of the experimental results and discussions. From the above discussions and various researches opinions, the paper uses the effective routing and clustering process is applied to eliminate the intermediate attack which is explained in the following section.

## III. PROPOSED METHODOLOGY

In this section discusses about the proposed clustering based energy efficient protocol for managing the security in the mobile ad ho networks. Initially the clusters have been formed in the network system by analyzing the interrelationship between the nodes. According to the relationship the clusters are formed and the cluster heads are continuously updating to eliminate the intermediate attacks. Then the detailed proposed methodologies are explained as follows which consists of three stages namely, cluster formation, routing and energy consumption which is explained as follows.

### 3.1 Cluster formation

The first stage of the secure communication system is cluster formation which is done with the help of the neighboring relationship based clustering protocol [12]. Initially the nodes are collected from the networks and the voting concept is applied to each node for all the neighboring nodes present in the network. For every node present in the network calculate the suitable property value for each node according to the voting value. From the obtained votes of each node, the cluster head has been chosen which follows the following rules.

**Rule 1:** Addition of the votes obtained from all the neighboring nodes in the network.

**Rule 2:** During the vote calculation process, the neighboring node who's having the higher residual energy which has the highest rank or vote else it has the lower rank.

Based on the above rules, the nodes present in the network votes are calculated using the particular node residual energy which is calculated as follows.

$$V(v_i, v_j) = \begin{cases} \dfrac{\left(\frac{e_j}{d_{ij}}\right)}{\sum_{d_{ij} \le R} d_{ik}} d_{ij} \le R, d_{ij} > R \end{cases} \quad (1)$$

Where, v is the votes of the neighbor in the network of sensor in the network $v_i, v_j$ using the rules R1 and R2. Then the total vote obtained by the node in the network is calculated as follows.

$$vote(v_i) = \sum_{d_{ij} \le R} v(v_i, v_j) \quad (2)$$

Based on the voting concept the particular node selects its neighboring node and the node which has obtain the maximum node which is selected as the cluster head. Then the cluster head selection message is sent to the node, if the node receives that message it does not add to any other cluster in the network. At the time of cluster head selection process, some of the criteria need to be followed like, if the node itself treated as the cluster head when it does not have any neighborhood node. So, the cluster heads are continuously changed according to the node voting concept. This cluster head only determines the path of information transmission between the nodes. So, the intermediate hackers like black hole and others difficult to find the optimal route between the source and destination in the mobile ad-hoc network. After selecting the cluster and cluster head, the optimal transmission route is determined by applying the fireflies based energy efficient routing protocol which reduces the energy consumption.

### 3.2 Routing and Energy Consumption Protocol

The next step is routing the information between the source and destination using the fireflies based energy efficient routing protocol [13] which utilize the multipath routing with the XOR based forward error correction. The forward error correction eliminates the redundancy of the data transmission also eliminates the delay present in the network. So, in this system the protocol uses the three different phases like initialization phase, primary path analyzing, discovery phase and the alternative path discovery phase. The first step is initialization phase in which the sensor node transmit the HELLO message to the neighboring nodes that includes the source ID, residual energy, link quality, hop count, free buffer. By using this information, the link cost is estimated as follows.

$$\alpha E_{resd,y} + \beta B_{buffer,y} + \gamma I_{interferrences,xy} \quad (3)$$

After estimating the link cost between the nodes, the path has been analyzed using the path discovery phase by sending the RREQ message to the neighboring nodes which is done by applying the equation 4.

$$Next\ hop = Max_{y \in Nx}\{\alpha E_{resd,y} + \beta B_{buffer,y} + \gamma I_{interferrence,xy} \quad (4)$$

In the equation (4), Nx is the neighbor set of the node x. $E_{resd,y}$ and $B_{buffer,y}$ represented as the residual energy and free buffer size of the neighbor y. $I_{interferrence,xy}$ is denoted as the signal to noise ratio between the node x and y. By using this process, the multiple paths has been constructed using the neighboring nodes and the alternative path has been generated with the help of the alternative paths discovery phase. The alternative path selects another path which is related to the primary path by sending the RREQ message to the most preferred neighboring node. The most preferred node has been selected by applying the fireflies' algorithm [14]. The algorithm analyzes the path according to the behavior of the fire flies flashing characteristics such as attractiveness and light intensity. The intensity value is estimated with the help of the maximum or minimum value of the node residual energy for the entire node. Further the attractiveness value is estimated using the distance between the nodes present in the network which is computed as using the Hausdorff distance measure.

$$d_H(X,Y) = \max\{\sup_{x \in X} \inf_{y \in Y} d(x,y), \sup_{y \in Y} \inf_{x \in X} d(x,y) \quad (5)$$

Sup- supremum, inf- infimum.

Where, $d_H(X,Y)$ - Similarity between the nodes.

Then the estimated node residual energy values are ranked according to the attractiveness and intensity value that helps to determine the nearer optimized node. The node having the highest attractiveness and intensity value that is considered as the highest priority. The highest ranked coefficient are selected which is used for further node or path selection process. From the selected nodes, the routing method, transmit the RREQ message, the node which accepts the first message that accepts during the path estimation process and the remaining nodes are discards. Then the number of path computation is determined as follows.

$$k = X_\alpha \sqrt{\sum_{i=1}^{N} p_i(1-p_i) + \sum_{i=1}^{N} p_i} \quad (6)$$

In the eqn (6), where, $X_\alpha$ is represented as the bound between the standard normal distribution for different levels of α. Pi is the probability of the successful delivery of the message.By using this process, the node has been successfully transmitting the information between the source and destination with secure manner because, before it sends the information, clusters are formed. In the cluster the highest priority node has been determined using the residual energy and the related voting concept which eliminates the intermediate attacks with efficient manner. At the time of transmission, the energy has been consumption by calculating the transmission delay. The transmission delay is measured by propagation delay of the particular message and the best path in the system. Thus the proposed system eliminates the intermediate black hole attack because the system efficiently utilizes the request message to the source and destination node with effective manner. Then the efficiency of the system is evaluated with the help of the experimental results which are discussed as follows.

## IV. EXPERIMENTAL RESULTS

In this section discusses about the experimental analysis about the proposed Fireflies based energy efficient routing protocol. The efficiency of the system is evaluated with the help of the NS2 tool based metrics like packet delivery ratio, energy utilization factor and percentage of attack free routing efficiency [15]. The estimated efficiency is compared with the different traditional methods like Qos aware peering routing method, localized multi objective routing method and Ad hoc On-demand Distance Vector (AODV). The simulation parameters value is listed in the table 1.

**Table 1 Simulation Parameters**

| Parameters | Values |
|---|---|
| Simulation Area | 250 $m^2$ |
| Number of nodes | 47 node (40 sensor node, 3 sink node, 6 relay node) |
| MAC | IEEE 802.15.4 |
| Packet size | 40 bytes |
| Transmission rate | 250kbps |
| Frequencies band | 420MHz,868MHz, 2.4GHz |
| Channel mode | Log shadowing wireless model |
| Evaluation Parameters | Delay, Energy Utilization factor, packet delivery ratio |
| Simulation time | 400sec |

According to the above table 1, the simulation parameters are used to analyze the proposed system efficiency. Then the performance metrics are discussed as follows.

### 4.1 Performance Metrics

In this section discusses about the few performance metrics like end to end delay, energy utilization factor, packet delivery ratio and the percentage of attack free routing efficiency.

### End to End Delay

Delay is the metric to determine the mean time to spend to transmit the message from source to destination. Then the delay has been calculated using the eqn 7 which contains both propagation delay and processing delay.

$$Delay = QD+PD+PGD \quad (7)$$

Where, QD- Queueing Delay, PD- Processing Delay, PGD is propagation delay.

### Energy Utilization Factor

The energy utilization factor is the metric that analyze the overall energy consumed by the manet network during the information transmission because the proposed system need to transmit the information with high security. So, the EUF is estimated as follows.

$$EUF = EU/TE *100 \quad (8)$$

### Packet Delivery Ratio

The ratio between the numbers of packets successfully sent to the destination from the source is called as the packet delivery ratio which is measured as follows.

PDR= No.of packets transmitted successfully/ No.of packets generated * 100 (9)

According to the above metrics, the efficiency of the system is discussed as follows. The figure 1 depicted that the end to end delay of the MANET network while transmitting the information. The system avoids the intermediate attacks also consumes minimum end to end delay. So, the proposed system consumes minimum end to end delay value while transmitting the data from source to destination when compared to the Qos aware peering routing method (QAPR), localized multi objective routing method (LMOR) and Ad hoc On-demand Distance Vector (AODV). The proposed system analyze the nodes in the present in the network and the priority of the neighboring node is estimated with effective manner, so it consumes only the minimum delay. The obtained delay metric is shown in the figure 1 as follows.

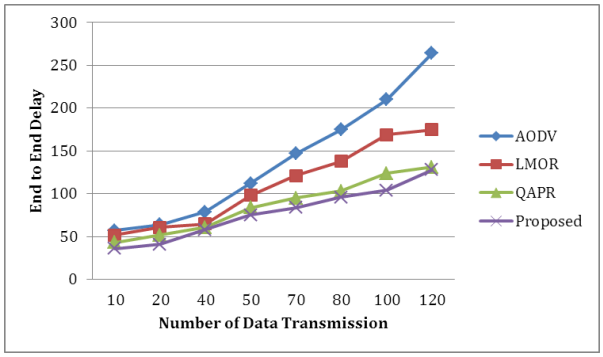


**Figure 1: End to End Delay**

From the above figure 1 clearly shows that the proposed system consumes minimum end to end delay while increasing the number of data transmission when compared to the existing methods. The minimum delay metric increases the packet delivery ratio which is shown in the figure 2.

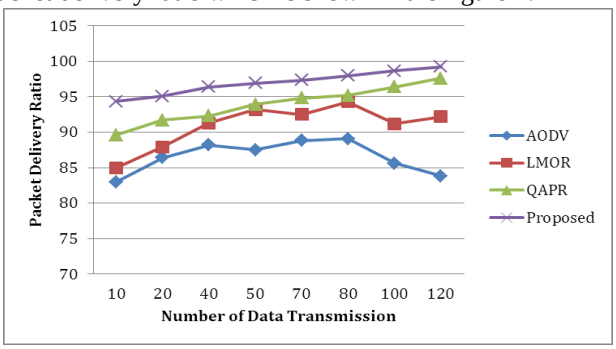


**Figure 2: Packet Delivery Ratio**

From the above figure 2 clearly shows that the proposed secure protocol method ensures the high packet delivery ratio while transmitting the data in the networks. Thus the maximum packet delivery ratio is consumed by the proposed system is 99.21%, AODV as 83.8%, LMOR as the 92.2% and QAPR as 97.6%. Even though the network has high packet delivery ratio which consumes minimum energy consumption which is shown in the figure 3.

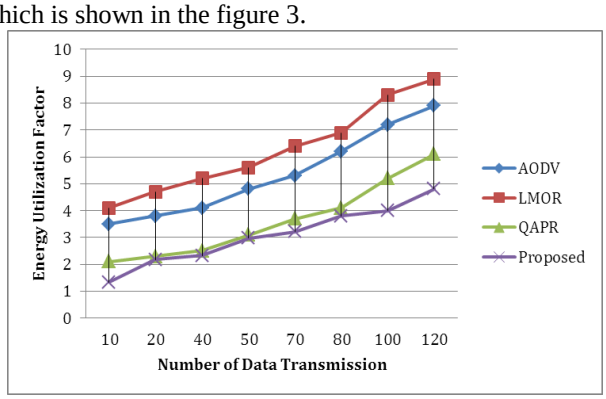


**Figure 3: Energy Utilization Factor**

Thus the proposed system successfully transmitting the information from the network with minimum delay and high packet delivery ratio by consuming the minimum energy. This leads to affected by any intermediate attacks but the proposed system successfully transmit the network by identifying the attack free routing path. Then the accuracy of the attack free routing path is shown in the figure 4.

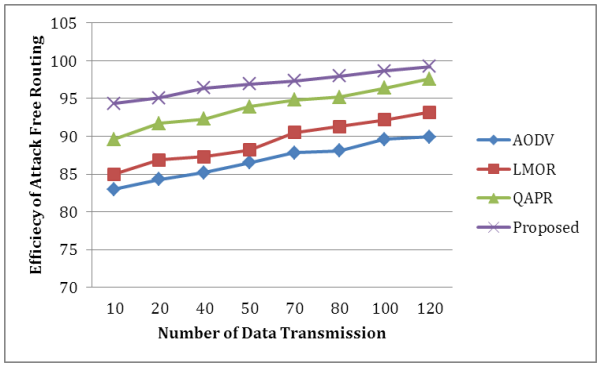


**Figure 4: Efficiency of Attack free Routing**

Thus the proposed system successfully transmitting the secure information in the mobile ad hoc network which is evaluated using the figure 4 also consumes minimum delay and high packet delivery ratio.

## V. CONCLUSION

Thus the paper introduces the neighboring relationship based fireflies energy efficient routing protocol for transmitting the data in the mobile ad hoc networks to overcome the security issues present in the packet transmission protocol. Initially the cluster has been formed by identifying the neighboring node relationship and voting concept according to the residual energy value that improves the cluster head selection process. During the clustering process, the cluster heads are changed depending on the neighboring node priority. From the selected cluster the RREQ message has been transmitted to all the neighboring nodes. Then the primary and alternative path is chosen depending on the firefly's behavior which reduces the redundant data also eliminate the intermediate attacks. Then the efficiency of the system is evaluated with the help of the experimental results in terms of using the end to end delay, packet delivery ratio, energy utilization factor and accuracy of the attack free routing which is compared with the AODV, LMOR and QAPR.

## REFERENCES

1. Ruay-Shiung Chang and Chia-JouKuo , " An Energy Efficient Routing Mechanism for Wireless Sensor Networks", Proceedings of the 20thInternational Conference on Advanced Information Networking and Applications , Vienna, Austria ,pp. 308 - 312 , April 2006.
2. Choi, P. Shah and S. K. Das," A Framework for Energy-Saving Data Gathering Using Two-Phase Clustering in Wireless Sensor Networks," Proceeding of the Mobile and Ubiquitous Systems, Boston, pp.203- 212,August 2004.
3. Sheela , G. Mahadevan, Mollifying the Effect of Cloning, Sink Hole and Black Hole Attacks in Wireless Sensor Networks using Mobile Agents with Several Base Stations, International Journal of Computer Applications (0975– 8887) Volume 55– No.9, October 2012.
4. MahaAbdelhaq, Rosilah Hassan, Mahamod Ismail, Raed Alsaqour, DaudIsraf, Detecting Sleep Deprivation Attack over MANET Using a Danger Theory –Based Algorithm, International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(3): 534-541 The Society of Digital Information and Wireless Communications, 2011 (ISSN: 2220-9085).
5. Gagandeep, Aashima, Pawan Kumar, Analysis of Different Security Attacks in MANETs on Protocol Stack A Review ,International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1,Issue-5, June 2012.
6. Tarek M. Mahmoud, Abdelmgeid A. Aly, Omar Makram,"A Modified AODV Routing Protocol to Avoid Black Hole Attack in MANETs", International Journal of Computer Applications (0975 – 8887), Volume 109 – No. 6, 2015.
7. Sonal R. Jathe, Dakhane, "Detection of Sinkhole Attack against DSR Protocol MANET", International Journal of Advanced Research in Computer Science and Software Engineering", Volume 2, Issue 4, April 2012.
8. Mohammad Al-Shurman, Seong-Moo Yoo, Seungjin Park, "Black hole attack in mobile Ad Hoc networks", ACM-SE 42 Proceedings of the 42nd annual Southeast regional conference, Pages 96-97.
9. Chaitas Shah,Prof. Manoj Patel, "Improving ZRP Protocol against Blackhole Attack", https://www.ijedr.org/papers/IJEDR1402103.pdf.
10. Dharman, G. Venkatachalam, "Detection of Gray Hole Attack in AODV for MANETs by using Secure Message Digest", South Asian Journal of Engineering and Technology Vol.2, No.17 (2016) 321–329.
11. PrachiGoyal, Chitvan Gupta, "An Approach for Security Measures of Black Hole Attack in MANET", International Journal of Emerging Trends in Science and Technology.
12. Qin and R. Zimmermann, "An Energy-efficient Voting-basedClustering Algorithm for Sensor Networks," Proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks(SNPD/SAWN'05), pp. 444-451 ,Maryland, USA, May 2005.
13. Younis and S. Fahmy, "Distributed Clustering for Scalable, Long Lived Sensor Networks," Proceedings of the 9th Annual International Conference on Mobile Computing and Networking, ACMMobiCom,San Diego, CA, September 2003.
14. [14] Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for mobile ad-hoc networks," in Proc. 9th International Conference on Network Protocols (ICNP).Riverside, California: IEEE, Nov. 2001, pp. 251–260.
15. [15] Mingqiang, E. R. Inn-Inn and K. G. S. Winston, "Analysis of Clustering and Routing Overhead for Clustered Mobile Ad Hoc Networks", (ICDCS'06) 26th IEEE International Conference on Distributed Computing Systems, pp.46, 2006.

## AUTHORS PROFILE

**M V S S Nagendranth** has Completed M.Tech in computer science and Engineering from SRM University, Chennai in the year 2005. He is currently pursuing Ph.D in Computer Science and Engineering, Hindusthan Institute of Technology and Science, Chennai. Currently working as a Associate Professor in Department of CSE at Sasi Institute of Technology & Engineering, Tadepalligudem, Andrapradesh. His research interests are Mobile Adhoc Networks, Data Security etc.. He is Life member of ISTE, CSI.

**Dr. A. Ramesh Babu** is working as Professor and Head, in the Department of Science & Humanities, Hindusthan Institute of Technology & Science, Chennai, India. He obtained Degrees in M. Tech, M.Sc., and Ph.D. His area of interest includes Graph theory, Operation Research, Discrete mathematics, Automata theory, Design and Analysis of Algorithm, Cryptography and Network Security, Data mining & Data ware housing, Graphics and Multimedia. He presented 30 papers in National and International Conferences and two papers in National Journals and 25 papers in International Journals.