

PERUSAL OF INTRUSION DETECTION AND PREVENTION SYSTEM ON A MANET WITH BLACK HOLE ATTACK: ISSUES AND CHALLENGES

Marepalli Radha¹ and C.V.Guru Rao²

¹Department of computer science and engineering, Adam's college, Paloncha, Telangana, India

²SR Engineering College, Warangal, Telangana, India

ABSTRACT:

MANET is a self configuring network of nodes which is a wireless . The nodes in this network move randomly .Mobility of nodes is more. The nodes are dynamic and infrastructure less ,self maintainable. In MANET there are many types of security attacks like Blackhole, greyhole attack, wormhole, jellyfish etc. When the MANET is under blackhole attack there is a loss of energy which is high at the node resulting in loss of battery backup and also excess of bandwidth may be consumed by the attacker. The attacker is an insider. Among various mobility models to generate mobility patterns the Random waypoint mobility model is used .To solve these issues an IDPS framework for MANET using image processing techniques under blackhole attack is proposed to detect the blackhole attack RREP by providing security services like authentication and confidentiality.

KEYWORDS :

AODV, BLACKHOLE ATTACK, IDPS, MANET, RWM IMAGE PROCESSING.

1. INTRODUCTION

MANET is a infrastructure less computing network. It is having freedom to act independently ,self ruling self configuring network ,arrange network of mobile nodes without method indiscriminately and formed without the need of a single authority[1].The increase of inexpensive small and having great powerful devices make MANET a fastest growing network. The uses of MANET are Military battlefield, Collaborative work, personal area network etc. The most demanding part of MANET is maintaining the routing information without loss of data. Routing is the method of selecting a path for traffic from source to destination. Routing Protocol is a principle or norm ,that controls how nodes select which path to send packets between computing devices in mobile Adhoc network. The movement of nodes in MANET is random. Hence, routing protocols are officially compulsory to manage routing information of nodes. MANET routing protocol is classified into three i.e. reactive protocol which is on demand and proactive protocol which is table driven and hybrid protocol. [2][3] Due to the absence of central cooperative effort for security on shared wireless medium makes MANET more exposed to digital/cyber attacks than wire line network. Attacks can be classified into two types:

1. **Passive Attacks:** Passive attacks does not disturb proper operation of network. Attackers snoop data exchanged in network without modifying the data. Confidentiality can be violated if an attacker is also able to interpret. This attack is difficult to be detected since the operation of network itself does not get affected.

2. Active Attacks: Active attacks are performed by the malicious nodes that carry some energy cost in order to perform the attacks. They involve some manipulation of data stream or creation of false stream.
3. Due to the Blackhole attack in Manet there are certain problems which need to be addressed [1]. There is a loss of energy at every node and excess consumption of bandwidth resource for which proposing a IDPS frame work with image processing technique to detect and prevent the blackhole attack. AODV protocol is used by the nodes to find routing between nodes. Generally there are three types of mobility models.

RANDOM WAY MOBILITY MODEL:

This model was first described by Einstein in 1926 to mimic irregular movements of particles in nature [5] which is known as Brownian Motion. It is a simple mobility model in which mobile node moves with zero pause time in a random directions and speeds. Random direction mobility model: In this mobility model mobile node chooses any random direction to travel until the boundary of edge is found. The Random Direction Mobility Model was created to overcome density waves in the average number of neighbors produced by the Random Waypoint Mobility Model.

The Random waypoint mobility model is chosen because it models the movement of nodes with maximum velocity. It is a baseline mobility model to evaluate the protocols in MANET. Therefore Random waypoint model is used in research work. [6, 7]

2. RELATED WORK

In [4] this section, related work of the proposed intrusion detection and prevention system literature reviewed.

2.1 MANET

MANET is a infrastructure less network which has no central organization Each and every node can be involved directly with every other node, hence it is difficult to discover and manage the faults. In MANET, the mobile nodes can move individually and in unfamiliar way. This dynamic network topology results in route changes, so frequent occurring network replacements and possibly packet losses [9]. In MANET, every node acts as a router and it will forward the packets to the other nodes in the network. The nodes can be connected to other nodes without central point. It is a self organizing capability which helps in finding the next hope neighbor to send the packets. The various applications of MANET such as defense, military, health care, agriculture etc. has made the researchers to analyze the routing protocols as data transmission is more effected due to mobile nodes. In MANET routing is challenging .The routing protocols define some rules to follow in order to communicate with other nodes. Routers in the network collect information about the topology by sharing the information among neighbors [1].

2.2 MANET ROUTING PROTOCOL - AODV

The Ad Hoc on-Demand Distance Vector Routing (AODV) [10] is also a reactive routing protocol which has two steps establishing and updating the routes. It keeps, a routing table to prevent the attack by comparing a sequence number. Whenever node wants to begin route discovery process, it includes its sequence number and fresh sequence number it has for destination. The intermediate nodes which receive the RREQ packet, will playback if it finds the sequence number higher then it will playback. A reverse route is setup from intermediate node to

International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 7, No 2, May 2018
the source by updating node's address from RREQ hence, in the bidirectional route is setup at the end of the request-response cycle between source and destination.. As long as the route is active when the packets are travelling in that path.. Once the source stops sending data packets, the links will be deactivated and deleted from the intermediate node routing tables. . After implementing this approach, there is vast decrease in packet drop and increase in throughput under black hole attack. But the delivery ratio of ADOV under attack is less. [6].

2.3 BLACKHOLE ATTACK

The functioning of MANET depends on partnership based mutual agreement and understanding among the nodes in the network, however some nodes may become malice and misbehave later. Black hole attack is one damaging attack which is caused by the malicious node [11].It will take advantage of the process of finding routes in reactive routing protocols. Whenever the source node broadcasts a route request a malicious node will respond claiming to have best path to the destination without checking the routing table, thereby redirecting the data packets through it and just discarding the packets without forwarding [12]. A malicious node can work independently to launch the attack, and this is referred as single blackhole attack or malicious can work as group then it is referred as cooperative black hole attack [13]

2.3.1BLACK HOLE ATTACK CATEGORIES

The black hole attack can also be classified into two categories based on the cause of the attack: Black hole attack caused by RREP and that caused by RREQ [14] as illustrated in Figure1. In Figure1, the black hole sends a forged RREP message pretending to have a fresh and short path to the destination. This means the black hole always returns a positive RREP even when it has no valid route to the destination. The data packets that are transmitted to the destination will therefore pass through a malicious node which will silently absorb or discard them. In Figure 1,the black hole sends a forged RREQ message to attack a target node in the network. This black hole pretends to be re broadcasting the RREQ packet that originated from a target node in the network. It then adds itself as the next hop in the route record, so the entire messages destined to the target node will pass through it and it will discard the messages.

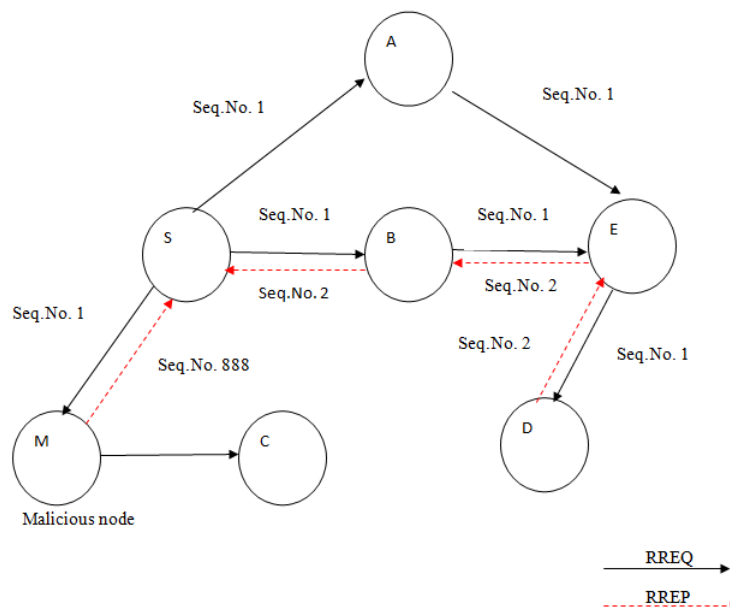


Figure 2 : Black hole attack via RREP

2.4 RANDOM WAYPOINT MOBILITY MODEL[5]

The Random Waypoint model is most commonly used mobility model in research community. The implementation of this mobility model is as follows: at every instant, a node randomly chooses a destination and moves towards it with a velocity chosen uniformly randomly from $[0, V_{max}]$, where V_{max} is the maximum allowable velocity for every mobile node. After reaching the destination, the node stops for a duration defined by the 'pause time' parameter. After this duration, it again chooses a random destination and repeats the whole process again until the simulation ends. This model is used in MANET as there are random changes in topology because of the random mobility of nodes will take place due to no central management and No boundaries.[1] The RPW model is the simplest and easiest to use. It is most commonly used model in research community. In Random way point mobility model, mobile nodes select the direction and speed randomly and independently to reach at the destination[16].

2.5 INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS) [4,17,16]

In today's world the whole system is going digital, it means everyone's data is being stored in digital machines instead of traditional way. Thus when digital communities are depending on computer technology to store valuable data/ secret information of a person in any counter of the world or nearby, it is necessary to keep the network safe from intruders/hackers/attackers. In order to keep it safe the data from these intruders, there emerged a mechanism called Intrusion Detection And Prevention System (IDPS). As the existing IDPS is not scalable a light weight IDPS may be developed, so as to decrease the overhead created by existing IDPS and a more scalable routing protocol might be used.

2.6 EXISTING INTRUSION DETECTION AND PREVENTION SYSTEM FOR MANET WITH BLACKHOLE ATTACKS

2.6.1. DETECTING AND PREVENTING BLACKHOLE ATTACK IN MANET ON AODV USING THRESHOLD VALUE[19]

The problem of Blackhole attack is discovered and solution is proposed to detect and prevent as follows: The method to find and prevent is by using the sequence numbers of source node and destination node investigating the difference between the nodes and verifying if the difference is higher than as a threshold value. Threshold value is the average of difference between the sequence number s in the routing table in each time slot. If sequence number is greater than threshold then it is to be throw away by joining it to the blacklist .when any node receives the RREP packet. It examines over the blacklist and no processing is done for the same. By simulation the results in referred paper are when the number of malice nodes increased then delivery ratio decreased and packet loss increased.[19]. Every time if any node receives the RREP packet, it has to look over the list, if the reply is from the blacklisted node; no processing is done for the same. It simply fails to consider the node and does not receive. Calculation of threshold overhead for every timeslot frequent checking of blacklist should be done.

2.6.2 PERFORMANCE ANALYSIS OF BLACKHOLE ATTACK PREVENTION AND DETECTION ALGORITHM IN MANETS[9,19]

The technique is given to identify multiple black holes cooperating with each other and discover the safe route by avoiding the attacks. It was assumed in the solution that nodes are already authenticated and therefore can participate in the communication. It uses Fidelity table where every node that is participating is given a fidelity level that will provide reliability to that node.

Any node having 0 values is considered as malicious node and is eliminated. [20] In future we can determine the effect of Black Hole attack on other routing protocols such as Dynamic source routing (DSR), Optimized Link State Routing (OLSR) and measure the performance of the network. To implement any detection techniques we need also consider performance factors such as Average Delay and Routing Overhead.

3. LITERATURE SURVEY

3.1 USING IMAGE PROCESSING PROVIDING BIOMETRIC –BASED USER AUTHENTICATION IN MANET

Biometric is an automatic identification verification system of an individual by his or her physiological or behavioral characteristics [21]. This system gives a solution to authentication in MANETs but it has its own quality and faults. We have Unimodal biometric and Multimodal biometric systems which provide more reliable authentication methods due to the combination of statistics biometric traits [23]. Unimodal biometrics has to face several challenges such as noise in sensed data, intra-class variations, inter-class similarities, etc. [22].

There are three different modes of system operation in multimodal biometrics system: serial mode, parallel mode, and hierarchical mode [22]. In serial mode of operation, one output of a biosensor will be used at one time. Therefore, multimodal biometric traits do not need to be acquired simultaneously, and the decision could be made before all biometric traits are received. The overall recognition time can be reduced, which is important for MANETs. In the parallel mode of operation, multimodal biometric traits have to be used simultaneously. The hierarchical mode of operation is suitable for the system using a large number of biometric traits. This paper will consider the serial mode of operation since it is suitable for continuous authentication in MANETs.

3.2 NORMAL OR BODY TEXT CONTINUOUS VERIFICATION USING MULTIMODAL BIOMETRICS

The goal is to have T. Sim et al. [28] proposed a continuous biometric authentication. The system was a multimodal biometric verification system which continuously verifies the presence of a logged-in user. But the system gives extra overhead on the resources required for multimodal fusion then compared to the conventional verification systems. The integration scheme used in this system is shown in Fig.2.

This has a security system in which resources need to be monitored continuously [29]. This method is used for biometric based continuous authentication for phone mobile communication system. This system gave access to e-signing, m-contracts in a secured authenticated approach. Based on various tests using the fusion techniques for biometric evidence combination, an efficient multi-modal biometric authentication was achieved on the Secure Phone PDA. The weighted error rate for the fusion technique is also calculated. Many existing IDS solutions are proposed for MANETs but they have their own significant limitations and weaknesses. Detecting all types of attacks is also not possible. Reducing the computational complexity is a challenging issue of all detection methods.

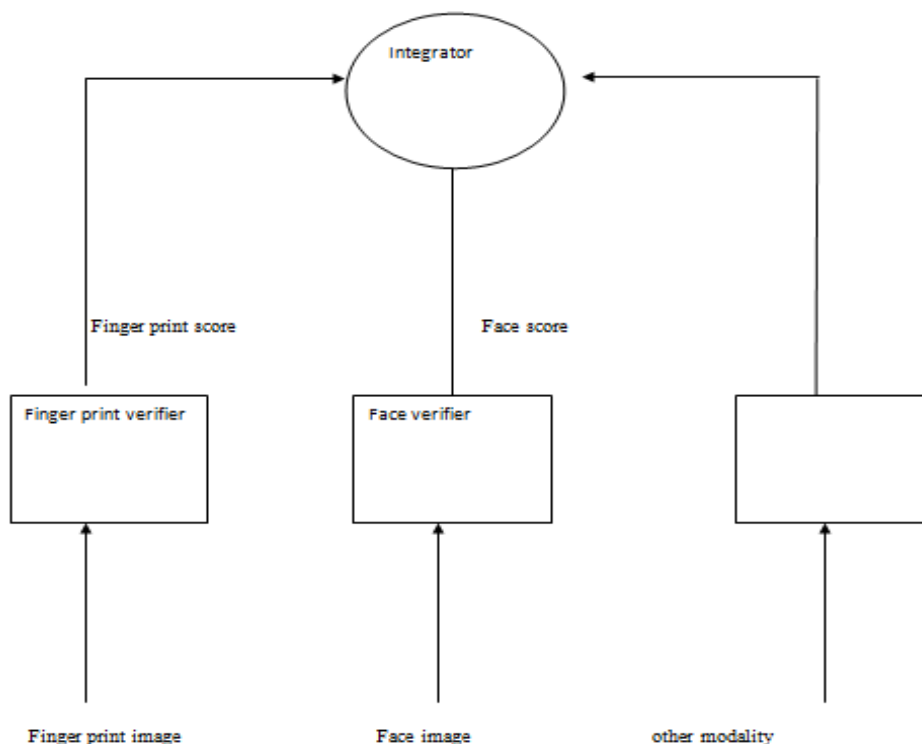


Figure 2: Integration Scheme

3.3 UNIMODAL BIOMETRIC ENCRYPTION KEY

To provide confidentiality, integrity and authentication, Hiteishi Diwanji and J.S. Shah [30] proposed Unimodal biometric encryption key method. In Unimodal biometric fingerprint DES algorithm is used and the encryption key is 48 bit for symmetric key. The feature set is created from fingerprint and 2*16 matrix is generated. And Crossover operation is performed on both the rows to produce a 48 bit key which is difficult to break for any cryptanalysis which ensures confidentiality and also integrity. In this for authentication can be done by using digital signature. In scheme suggests generation of key on both sides (sender and receiver) is done using same formula, so stealing cannot be possible.. This scheme withstands all the cryptanalysis attack because every time different feature set is used so cryptanalysis will not be able to find out the key even if intruder has got cipher text-plaintext pair. But still these models are not too much efficient and robust so they can be applied on real conditions effectively. Fingerprints can be forged and collecting and matching face prints is time consuming and complex. Veins and Vein patterns are not yet explored too much for MANETs. Some areas like pattern recognition in MANETs, securing and maintaining the biometric database in MANET, combining secure routing with authentication process, designing efficient cryptographic algorithms for MANETs and secure collection and maintenance of up to date audit data in intrusion detection system are still to be explored efficiently.

4. CONCLUSION & FUTURE WORK

The various techniques are studied for detection of blackhole attack in AODV routing protocol. By studying the various techniques, new methodology IDPS frame work will be proposed for prevention of attack. In proposed IDPS the focus is on prevention of blackhole attack by providing authentication and confidentiality security services. The proposed framework for IDPS smartly uses image processing techniques like Biometric technique for authentication and

International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 7, No 2, May 2018

Unimodal biometric encryption key provide confidentiality to save the bandwidth of the network and battery of genuine node. simulation results for the same would be captured and analyzed to show the effectiveness of the proposed prevention mechanism Without knowledge of the identity of intermediate nodes in operation, it is difficult to decide which nodes are trustworthy in MANET network . To provide the security in the MANET by identifying nodes using image processing technique as mentioned above are deployed to provide authentication of nodes and confidentiality in future enhancement.

REFERENCES

- [1] Ankur O. Bangand Prabhakar L. Ramteke. 2013. MANET: History,Challenges And Application International Journal of Application or Innovation in Engineering & Management Vol.2 Issue 9.
- [2] V.G.Muralishankar and Dr. E. George Dharma Prakash Raj. 2014 Routing Protocols for MANET: A Literature Survey. International Journal of Computer Science and Mobile Applications Vol.2 Issue pg. 18-24
- [3] parvinder Kaur, Dr. Dalveer Kaur & Dr. Rajiv Mahajan. 2015. The Literature Survey on Manet Routing Protocols and Metrics. Global Journal of Computer Science and Technology Volume 15 Issue 1 Version 1.0
- [4] Bilal Maqbool Beigh , Uzair Bashir and Manzoor Chachoo . 2013. Intrusion Detection and Prevention System: Issues and Challenges.International Journal of Computer Applications (0975 – 8887) Volume76 No.17.
- [5] Muhammad Amir Nisar, Amir Mehmood and Adnan Nadeem. 2013 A Review and Performance Analysis of Mobility Models for MANETs: A Case Study. Federal Urdu University of Arts Science & Technology, Karachi, Pakistan, Conference Paper.
- [6] M. Sandhya Rani, R .Rekha, K.V.N.Sunitha, Performance Evaluation of MANET Routing Protocols Using Random Waypoint Mobility Model. International Journal of Advanced Research in Computer Science and Software Engineering 4(4), April - 2014, pp. 1293-1299
- [7] AnuBala, Jagpreet Singh and MunishBansal “Performance Analysis of MANET under Blackhole Attack” First International Conference on Network and Communication 2009
- [8] Bilal Maqbool Beigh , Uzair Bashir and Manzoor Chachoo . 2013. Intrusion Detection and Prevention System: Issues and Challenges.International Journal of Computer Applications (0975 – 8887) Volume76 No.17.
- [9] Jeoren Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demester “ An Overview of Mobile ad hoc Networks: Applications &Challenges .“
- [10] C.E. Perkins, E.M. Royer, S.R. Das, Ad hoc on demand distance vector (AODV) routing, in: IEEE WMCSA, 1999
- [11] M. Medadian, A. Mebadi and E. Shahri: "Combat with black hole attack in AODV routing protocol",Proceedings of the 9th IEEE Malaysia International Conference on Communications (MICC), pp. 530-535, 2009
- [12] Vani and D. S. Rao: "Removal of blackhole attack in ad hoc wireless networks to provide confidentiality security service", International Journal of Engineering Science and Technology,Vol. 3, pp.2377-2384, 2011.
- [13] P. K. Singh and G. Sharma: "An efficient prevention of black hole problem in AODV routing protocol in MANET", Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications(TrustCom), pp. 902-906, 2012.
- [14] M. K. J. Kumar and R. S. Rajesh: "Performance Analysis of MANET Routing Protocols in Different Mobility Models", IJCSNS International Journal of Computer Science and Network Security, Vol. 9 No.2, pp. 22-29, 2009.
- [15] Muhammad Amir Nisar, Amir Mehmood and Adnan Nadeem. 2013 A Review and Performance Analysis of Mobility Models for MANETs: A Case Study. Federal Urdu
- [16] Dr. A. Francis Saviour Devaraj , Mr. Akalu Assefa , TO PROPOSE A FRAMEWORK – IDPS FOR A MANET UNDER FLOODING ATTACK, JournalOf Advanced Research in Engineering & Management (IJAREM)ISSN: 2456-2033 || PP. 34-44
- [17] B. Zhang H.T. Mouftah "QoS Routing for Wireless Ad Hoc Networks: Problems Algorithms and Protocols" IEEE Communications Magazine vol. 43 no. 10 pp. 110-117 Oct. 2005.

- International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 7, No 2, May 2018
- [18] Ravi Kant, Sunil Gupta, A Literature Survey on Black Hole Attacks on AODV Protocol in MANET, International Journal of Computer Applications (0975 – 8887) Volume 80 – No 16, October 2013
- [19] SaritaBadiwal, AishwaryKulshrestha, NeerajGarg, Analysis of Black Hole Attack in MANET using AODV Routing Protocol, International Journal of Computer Applications (0975 –8887)Volume 168 – No.8, June 2017
- [20] Prof.M.B.Lonare¹, Anil Choudhary², Chehel Sharma³, Ershad Mulani⁴, Harish Yadav⁵, Prevention and Detection of Blackhole Attack in MANET using Modified AODV Protocol, International Journal of Advance Engineering and Research Development Volume 4, Issue 4, April -2017
- [21] Q. Xiao, “A biometric authentication approach for high security ad-hocnetworks,” in Proc. IEEE Info. Assurance Workshop, West Point, NY,June 2004.
- [22] Ross and A. K. Jain, “Multimodal biometrics: an overview,” in Proc.12th European Signal Proc. Conf., Vienna, Austria, 2004.
- [23] Ross and A. K. Jain, “Information fusion in biometrics,” Pattern Recognition Lett., vol. 24, pp. 2115-2225, Sept. 2003.
- [24] C.E. Perkins, E. M. Belding-Royer, and S. R.Das, “AdHoc On-Demand Distance Vector Routing”, IETF RFC 3561,July 2003.
- [25] M.Ambika , R.V.Natraj Intrusion Detection and Continuous Authentication using Multimodal Biometrics in MANETS – A Survey, International Journal of Computer Applications (0975 – 8887) International Conference on Innovations In Intelligent Instrumentation, Optimization And Signal Processing “ICIIOSP-2013”
- [26] S. Bu, F. Yu, X. Liu, P. Mason and H. Tang, “Distributedcombined authentication and intrusion detection with data fusionin high-security mobile ad hoc networks,” IEEE Transactions onVehicular Technology, vol 60 no.3 pp. 1025–1036, March 2011.
- [27] H.Nakayama, S.Kurosawa, A.Jamalipour, Y. Nemoto, N.Kato, "A Dynamic Anomaly Detection Scheme for AODVBasedMobile Ad Hoc Networks," IEEE Transactions onVehicular Technology, vol.58, no.5, pp.2471-2481, Jun 2009.
- [28] Sim T, Zhang S, R.Janakiraman and S.Kumar, “Continuous verification using multimodal biometrics,” IEEE Trans. Pattern Anal. Mach. Intell.2007; vol. 29, pp. 687-700.
- [29] Korman J, A C Morris, D Wu and S.A.Jassim, “Multi-modal biometrics authentication on the secure phone PDA,” in Proc. 2nd Workshop Multimo
- [30] Hiteishi Diwanji and J.S. Shah. “Enhancing Security in MANET through Unimodal Biometric Encryption Key” in IEEE, December 2011.

AUTHORS DETAILS:

M.Radha is currently Working as a Associate professor for 15 years She received her B.Tech degree from Swami Ramanadha institute of science and technology ,Nalgonda and M.Tech degree from Karshak Engineering college ,Hyderabad in 2009.Her research lies in the field of wireless networking especially in MANET.



Dr.C.V.Guru Rao working as a professor Director over a period of 32 years in his Service. He was awarded Ph.D degree in Computer science and Engineering from Indian InstituteofTechnology,Kharagpur,west Bengal,India.

