Security Mechanisms for MANET Routing Protocols Using Random Waypoint Models in Cryptography Analysis

[1]M.Sreerama Murty, [2]C.Dastagiraiah, [3]R.Ashok Kumar

[1]Department of Computer Science and Engineering
Sai Spurthi Institute of Technology,Khamamm,Andhra Pradesh,India
[2]Department of Information Technology
Sai Spurthi Institute of Technology,Khamamm,Andhra Pradesh,India

Abstract

A Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes forming a self-configuring network without using any existing infrastructure. Security problems due to their unique characteristics such as mobility, dynamic topology and lack of central infrastructure support. In conventional networks, transmitting the data from source to destination in multiple ways to require a certificate authority (CA) or trusted third party to provide security services including digital certificates, authentication and encryption. A Network model that includes pause times between changes in destination and speed. A node begins with a point in one location for a certain period of time. Once this time expires, the node chooses a random destination in the simulation area and a speed that is uniformly distributed between minimum and maximum speed. The node then travels toward the newly chosen destination at the selected speed. Then, the node pauses for a specified time period before starting the process again. While during this process in a network data can't be transferred under security measures. If so apply the security mechanisms in a network to secure.

Keywords : *MANET,Security,Simulation,Mobility,Topology*

1. Introduction

The main reasons for implementing the security mechanisms to improve security levels in a random network. To evaluate the performance and security levels using random waypoint model. In a random waypoint network have different nodes, to reach the data from source to destination using random selection and apply the shortest path mechanisms. while during this process the data can't be transferred securely. by using the encryption and decryption algorithms for providing the authentication in data transmission. In cryptographic systems, the term key refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to individuals, who have the corresponding key to recover the information. Consequently, the term key management refers to the secure administration of keys to provide them to users where and when they are required. With public-key cryptography, keys come in pairs of matched "public" and "private" keys. The public portion of the key pair can be distributed in a public manner without compromising the private portion, which must be kept secure. An operation done with the public key can only be undone with the corresponding private key.

2. Literature Survey

2.1 The paper ".**A Distributed and Scalable Time Slot AllocationProtocol for Wireless Sensor Networks"** by Chih-Kuang Lin, Student Member, IEEE, Vladimir I. Zadorozhny, Member, IEEE, Prashant V. Krishnamurthy, Member, IEEE, Ho-Hyun Park, and Chan-Gun Lee. This paper drive's There are performance deficiencies that hamper the deployment of Wireless Sensor Networks (WSNs) in critical monitoring applications. Such applications are characterized by considerable network load generated as a result of sensing some characteristics of the monitored system. Excessive packet collisions lead to packet losses and retransmissions, resulting in significant overhead costs and latency. In order to address this issue, we introduce a distributed and scalable scheduling access scheme that mitigates high data loss in data-intensive sensor networks and can also handle some mobility. Our approach alleviates transmission collisions by employing virtual grids that adopt Latin Squares characteristics to time slot assignments. We show that our algorithm derives conflict free time slot allocation schedules without incurring global overhead in scheduling. Furthermore, we verify the effectiveness of our protocol by simulation experiments. The results demonstrate that our technique can efficiently handle sensor mobility with acceptable data loss, low packet delay, and low overhead.

2.2 The paper **"Efficient Data Collection in Wireless Sensor Networks with Path-Constrained Mobile Sinks** by Shuai Gao, Hongke Zhang, and Sajal K. Das, Senior Member, IEEE , This paper drive's Recent work has shown that sink mobility along a constrained path can improve the energy efficiency in wireless sensor networks. However, due to the path constraint, a mobile sink with constant speed has limited communication time to collect data from the sensor nodes deployed randomly. This poses significant challenges in jointly improving the amount of data collected and reducing the energy consumption. To address this issue, we propose a novel data collection scheme, called the Maximum Amount Shortest Path (MASP), that increases network throughput as well as conserves energy by optimizing the assignment of sensor nodes. MASP is formulated as an integer linear programming problem and then solved with the help of a genetic algorithm. A two-phase communication protocol based on zone partition is designed to implement the MASP scheme. We also develop a practical distributed approximate algorithm to solve the MASP problem. In addition, the impact of different overlapping time partition methods is studied. The proposed algorithms and protocols are validated through simulation experiments using OMNET++.

2. 3 The paper **"Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients" by** Chan Chen, Student Member, IEEE, and Michael A. Jensen, Fellow, IEEE

This paper drive's When implementing data encryption and decryption in a symmetric cryptosystem, secure distribution of the secret key to legitimate nodes can be a challenge. In this paper, we consider establishing secret keys using the common wireless channel, with particular emphasis on the spatial and temporal correlations of the channel coefficients. Specifically, we investigate the influence of channel correlation on the bound of the key size generated from the common channel using a simple single-input single-output channel model, and we verify the existence of a sampling approach able to generate a key using the minimum possible sampling window. We also explore de correlation of the channel coefficients in a multiple-input multiple-output channel, and we use a statistical independence test to demonstrate that this process cannot be separated into spatial and temporal de correlation processes. The insights gained from these studies assist in the development of a practical key generation protocol based on a published channel coefficient quantization method and incorporating flexible quantization levels, transmission of the correlation eigenvector matrix, and LDPC coding to improve key agreement in an authenticated public channel. Finally, we present simulations with real channel measurements that solidify the fundamental conclusions.

2.4 The paper "**Security Games for Vehicular Networks** by Tansu Alpcan, Member, IEEE, and Sonja Buchegger, Member, IEEE.This paper drive's the Vehicular networks (VANETs) can be used to improve transportation security, reliability, and management. This paper investigates security aspects of VANETs within a game-theoretic framework where defensive measures are optimized with respect to threats posed by malicious attackers. The formulations are chosen to be abstract on purpose in order to maximize applicability of the models and solutions to future systems. The security games proposed for vehicular networks take as an input centrality measures computed by mapping the centrality values of the car networks to the underlying road topology. The resulting strategies help locating most valuable or vulnerable points (e.g., against jamming) in vehicular networks. Thus, optimal deployment of traffic control and security infrastructure is investigated both in the static (e.g., fixed roadside units) and dynamic cases (e.g., mobile law enforcement units). Multiple types of security games are studied under varying information availability assumptions for the players, leading to fuzzy game and fictitious play formulations in addition to classical zero-sum games. The effectiveness of the security game solutions is evaluated numerically using realistic simulation data obtained from traffic engineering systems.

3. Analysis of Random Waypoint Model

It became a 'benchmark' mobility model to evaluate the MANET routing protocols, because of its simplicity and wide availability. The Random waypoint model is a random-based mobility model used in mobility management schemes for mobile communication systems. The mobility model is designed to describe the movement pattern of mobile users, and how their location, velocity and acceleration change over time. Mobility models are used for simulation purposes when new network protocols are evaluated. In random-based mobility simulation models, the mobile nodes move randomly and freely without restrictions. To be more specific, the destination, speed and direction are all chosen randomly and independently of other nodes. This kind of model has been used in many simulation studies. Two variants, the Random walk model and the Random direction model are variants of the Random waypoint model

The implementation of this mobility model is as follows: as the simulation starts, each mobile node randomly selects one location in the simulation field as the destination. It then travels towards this destination with constant velocity chosen uniformly and randomly from [0,V], where the parameter V is the maximum allowable velocity for every mobile node. The velocity and direction of a node are chosen independently of other nodes. Upon reaching the destination, the node stops for a duration defined by the 'pause time' parameter . If T=0, this leads to continuous mobility. After this duration, it again chooses another random destination in the simulation field and moves towards it. The whole process is repeated again and again until the simulation ends

In the Random Waypoint model, V and T are the two key parameters that determine the mobility behavior of nodes. If the V is small and the pause time T is long, the topology of Ad Hoc network becomes relatively stable. On the other hand, if the node moves fast (i.e., is large) and the pause time T is small, the topology is expected to be highly dynamic. Varying these two parameters, especially the V parameter, the Random Waypoint model can generate various mobility scenarios with different levels of nodal speed. Therefore, it seems necessary to quantify the nodal speed.

4. Methodologies

The following Methodologies for implementing the Performance and Security

4.1 Route Map

When a source node wants to send packets to a destination to which it does not have a route, it initiates a Route Discovery by broadcasting a route request. The node receiving a route request checks whether it has a route to the destination in its cache. If it has, it sends a route reply to the source including a source route, which is the concatenation of the source route in the route request and the cached route. If the node does not have a cached route to the destination, it adds its address to the source route and rebroadcasts the route request. When the destination receives the route request, it sends a route reply containing the source route to the source. Each node forwarding a route reply stores the route starting from itself to the destination. When the source receives the route reply, it caches the source route.

4.2 Route Maintenance

Route Maintenance, the node forwarding a packet is responsible for confirming that the packet has been successfully received by the next hop. If no acknowledgement is received after the maximum number of retransmissions, the forwarding node sends a route error to the source, indicating the broken link. Each node forwarding the route error removes from its cache the routes containing the broken link.

4.3 Route Update

When a node detects a link failure, our goal is to notify all reachable nodes that have cached that link to update their caches. To achieve this goal, the node detecting a link failure needs to know which nodes have cached the broken link and needs to notify such nodes efficiently. Our solution is to keep track of topology propagation state in a distributed manner. The algorithm starts either when a node detects a link failure or when it receives a notification.

In a cache table, a node not only stores routes but also maintain two types of information for each route:, how well routing information is synchronized among nodes on a route; and which neighbor has learned which links through a route reply Each node gathers such information during route discoveries and data transmission, without introducing additional overhead. The two types of information are sufficient; because *each* node knows for each cached link which neighbors have that link in their caches.

4.3 Message Transmission

The Message transfer relates with that the sender node wants to send a message to the destination node after the path is selected and status of the destination node through is true. The receiver node receives the message completely and then it sends the acknowledgement to the sender node through the router nodes where it is received the message.

4.4 Packet Delivery ratio

Packet Delivery Ratio(PDR): The number of data packets sent from the source to the number of received at the destination.

PDR = (control packets sent-delivery packet sent) / control packets sent

4.5 Generating Keys

4.6 Random Key Generation

Good keys are random-bit strings generated by some automatic process. if the key is 64 bits long, every possible 64-bit key must be equally likely. generate the key bits from either a reliable random source or a cryptographically secure pseudo-random –bit generator.

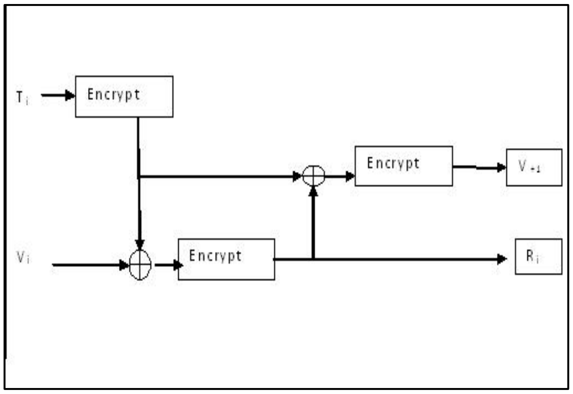


Fig: 4.5.21 X9.17 key generation

This does not generate easy-to-remember keys ;it is more suitable for generating session keys or pseudo-random numbers within a system. the cryptography algorithm used to generate keys is triple DES ,but it could just as easily be any algorithm.

Let $E_K[X]$ be triple-DES, encryption of X with Key K.this is a special key reserved for secret key generation .Vo is a secret 64-bit seed is a timestamp. To generate the random key R_i calculate:

$$R_i=E_k(E_k(T_i)\boldsymbol{\theta}Vi)$$

To generate V_{i+1} calculate:

$$V_{i+1}= E_k(E_k(T_i)\boldsymbol{\theta}\ R_i)$$

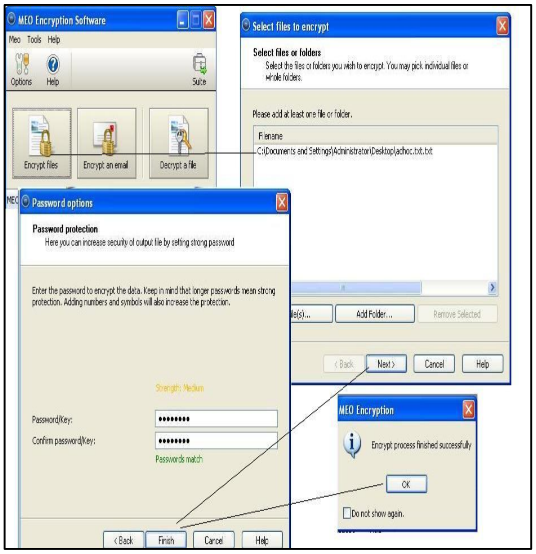
To turn $R_{i\text{ into DES}}$ key, simply adjust every eighth bit for parity. If you need a 64-bit key, use it as is. If you need a 128-bit key, generate a pair of keys and concatenate them together.

In cryptographic systems, the term key refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to individuals, who have the corresponding key to recover the information. Consequently, the term key management refers to the secure administration of keys to provide them to users where and when they are required. A major advance in cryptography occurred with the invention of public-key cryptography. The primary feature of public-key cryptography is that it removes the need to use the same key for encryption and decryption. With public-key cryptography, keys come in pairs of matched “public” and “private” keys. The public portion of the key pair can be distributed in a public manner without compromising the private portion, which must be kept secure. An operation done with the public key can only be undone with the corresponding private key. These encryption algorithms typically work fast and are well suited for encrypting blocks of messages at once. The most encryption methods are DEA (Data Encryption Algorithm) which is specified within the DES (Data Encryption Standard). Triple DES is a more reliable version while AES (Advanced Encryption Standard).Asymmetric algorithms are more commonly known as Public-key cryptography.

5. Experimental Results

5.1 Data Encryption

The below diagram derives, when the data is transmitted before the network to provide the encrypt the file and transmit source to destination.


MEO Encryption Software
Meo Tools Help
Options Help Suite
Encrypt files Encrypt an email Decrypt a file
Select files to encrypt
Filename
ile(s)... Add Folder... Remove Selected
‹ Back Next › Cancel Help
Password options
Strength: Medium
‹ Back Finish Cancel Help
MEO Encryption
OK

Select files or folders
Select the files or folders you wish to encrypt. You may pick individual files or whole folders.

Please add at least one file or folder.

C:\Documents and Settings\Administrator\Desktop\adhoc.txt.txt

Password protection
Here you can increase security of output file by setting strong password

Enter the password to encrypt the data. Keep in mind that longer passwords mean strong protection. Adding numbers and symbols will also increase the protection.

Password/Key: ••••••••
Confirm password/Key: ••••••••
Passwords match

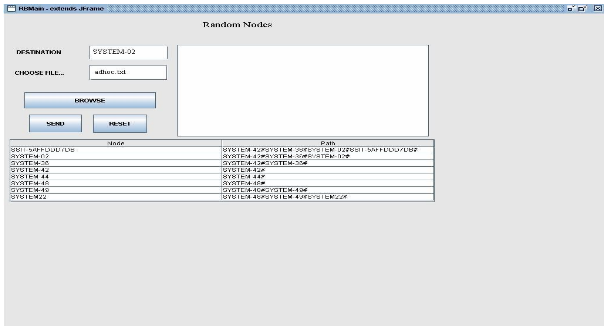
Encrypt process finished successfully

□ Do not show again.

Fig 5.1 Data Encryption For Before the data Transmission in a Network

5.2 Data Transmission

The given picture represents the nodes are updated in randomly in a network.



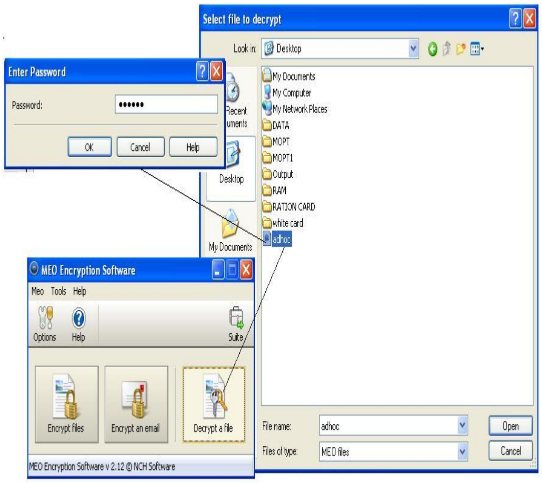
DESTINATION SYSTEM-02
CHOOSE FILE... adhoc.txt

Node	Path
SSIT-5AFFDDD7DB	SYSTEM-42#SYSTEM-36#SYSTEM-02#SSIT-5AFFDDD7DB#
SYSTEM-02	SYSTEM-42#SYSTEM-36#SYSTEM-02#
SYSTEM-36	SYSTEM-42#SYSTEM-36#
SYSTEM-42	SYSTEM-42#
SYSTEM-44	SYSTEM-44#
SYSTEM-48	SYSTEM-48#
SYSTEM-49	SYSTEM-48#SYSTEM-49#
SYSTEM22	SYSTEM-48#SYSTEM-49#SYSTEM22#

Fig: 5.2 Data transmission from selected node to destination node.

5.3 Decryption after Data Transmission

Given picture represents, when the data is reached from source to destination should decrypt the file.



Look in: Desktop

Password: ••••••

File name: adhoc
Files of type: MEO files

MEO Encryption Software v 2.12 © NCH Software

Fig: 5.3 Decryption

5.4 Response time between and Dynamic nodes and Static Nodes

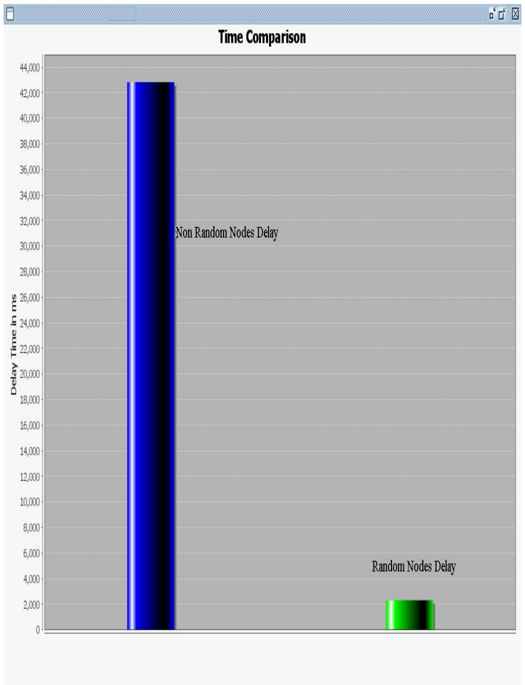


Fig: 5.4 Delay between data transmission.

6. Conclusion

In the general network, data can’t be transferred securily.when apply the cryptography techniques, we resolve the problems in the network. While transmitting the data over the network, we provide security and along corresponding time. So, data can’t be hack. In these security mechanisms to overcome the traffic problems in a random based network.

7. Future work

The future work of this paper is to implement the better cryptography algorithms for transferring the data in various network models.

References

[1] C.E. Perkins, E.M. Royer & S. Das, Ad Hoc On Demand Distance Vector (AODV) Routing,IETFInternet draft, draft-ietf-manet-aodv-08.txt, March 2001

[2] Tracy Camp, Jeff Boleng and Vanessa Davies, “ A survey of Mobility Models for Ad hocNetwork Research”, Wireless Communications and Mobile computing: A special issue on Adhoc network Research, vol 2, No5, pp. 483-502, 2002

[3] Naski, S. 2004. ‘Performance of Ad Hoc Routing Protocols: Characteristics and Comparison.’Seminar on Internetworking, Helsinki University of Technology, Finland.

[4] D. Johnson, D. Maltz. “Dynamic source routing in ad hoc wireless networks,” In T. Imelinsky and H. Korth, editors, Mobile Computing, pages 153-181. Kluwer Academic Publishers, 1996.

[5] S. Lee, M. Gerla, and C. Chiang. “On-Demand Multicast Routing Protocol.” IEEE WirelessCommunications and Networking Conference (WCNC’99), 1999.

[6] Ahmed S. and Ramani A. K., “Exploring the Requirements for QoS in Mobile Ad hoc Networks,”Journal of Information & Communication Technology Vol. 1, No. 2, (Fall 2007) 01-09

[7] Aziz S. R. A., Endut N. A., Abdullah S. and Daud M. N. M., “Performance evaluation of AODV, DSR and DYMO routing protocol in MANET”, CSSR 08-09, 14 - 15 March 2009.

[8] Perkins C. E. and Royer E. M., “Ad-Hoc On-Demand Distance Vector Routing, Mobile Computing Systems and Applications,” Proc. IEEE Workshop Mobile Computing Systems & Applications (WMCSA ’99), pp. 90-100, 1999.

[9] J. Broch, D. Maltz, D. Johnson, Y.-C. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In Proc. 4th ACM MobiCom, pp. 85–97, 1998.

[10] IEEE Computer Society LAN MAN Standards Committee. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, IEEE Std 802.11-1997. The IEEE, New York, New York, 1997.

[11] D. Johnson and D. Maltz. Dynamic Source Routing in ad hoc wireless networks. In Mobile Computing, T. Imielinski and H.Korth, Eds, Ch. 5, pp. 153–181, Kluwer, 1996

[12] C. Perkins, E. Royer, and S. Das. Ad hoc On-demand Distance Vector (AODV) Routing, RFC 3561. http://www.ietf.org/rfc/rfc3561.txt, July 2003.

[13] G. Lin, G. Noubir, and R. Rajaraman, “Mobility models for ad hoc network simulation,” in Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM ’04), vol. 1, pp. 454–463, Hongkong, March 2004.

[14] T.Camp,J.Boleng, and V.Davies,A Survey of Mobility Models for Ad Hoc Network Research,in Wireless communication and mobile computing:Special issue on Mobnile Ad Hoc Networking:Research,Trends and Applications,vol.2no .5 pp,483-502,2002

[15] Y.-C. Hu and D. B. Johnson. Caching Strategies in On-Demand Routing Protocols for Wireless Ad Hoc Networks, in Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000), ACM, Boston, MA, August 2000.

[16] D. M. Blough, G. Resta and P. Santi, A statistical analysis of the long-run node spatial distribution in mobile ad hoc networks, in Procedding of ACM International Workshop on Modeling, Analysis and Simulation of Wireless and Mobile Systems(MSWiM), Atlanta, GA, Sep. 2002.

[17] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, and M. Degermark, Scenario-based performance analysis of routing protocols for mobile ad-hoc networks, in

International Conference on Mobile Computing and Networking (MobiCom'99), 1999, pp. 195--206.

[18] R. Folio, J. B. Cain, and S. Kota, “Challenges in the verification of mobile ad hoc networking systems,” International Journal of Wireless Information Networks, vol. 14, no. 2, pp. 107–120, 2007.

[19] E. Hyyti¨a and J. Virtamo, “Random waypoint mobility model in cellular networks,”WirelessNetworks, vol. 13, no. 2, pp. 177–188, 2007

[20] P. S. Mogre, M. Hollick, N. d’Heureuse, H. W. Heckel, T. Krop, and R. Steinmetz, “A graph-based simple mobility model,” in Proceedings of the 4th Workshop on Mobile Ad-Hoc Networks (WMAN ’07), pp. 421–432, Bern, Switzerland,February-March 2007.

[21] S. Gowrishankar, T. G. Basavaraju, and S. K. Sarkar, “Effect of random mobility models pattern in mobile ad hoc networks,”International Journal of Computer Science and Network Security, vol. 7, no. 6, pp. 160–164, 2007.

[22] N. Aschenbruck, E. Gerhards-Padilla, and P. Martini, “A survey on mobility models for performance analysis in tactical mobile networks,” Journal of Telecommunications and Information Technology, vol. 2, pp. 54–61, 2008.

Acknowledgements

The authors would like to thank the anonymous reviewers for their careful reading and insightful comments that have helped in improving of this paper.

M.Sreerama Murthy Recived M.Tech in Computer Scince and Engineering from University College of Engineering ,JNTU,Kakinada.B.Tech in Information Technology from Sai Spurthi Institute of Technology,Khammam Affiliated to JNTUH. And now presently working as Assistant Professor in Sai Spurthi Institute of Technology,Khammam.His research interests includes Mobile Computing,Image Processing,DataMining and Embedded Systems.

C.Dastagiraiah Recived M.Tech in Computer Scince and Engineering from University College of Engineering,Acharya Nagarjuna University.B.Tech in Computer Scince and Engineering from ACET,Allagadda affiliated to JNTUH. And now presently working as Associate Professor and Head of the Department of IT in Sai Spurthi Institute of Technology,Khammam.His research interests includes Mobile Computing,Image Processing,DataMining and Embedded Systems.

R.Ashok Kumar Pursuing M.Tech in Computer science Engineering from Mother Theresa Institute of Science and Technology,Sathupally affiliated to JNTUH. B.Tech in CSE from Sai Spurthi Institute of Technology,Khammam Affiliated to JNTUH. And now presently working as Assistant Professor in Sai Spurthi Institute of Technology,Khammam.His research interests includes Mobile Computing,Image Processing,DataMining and Embedded Systems