International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 1 –NOVEMBER 2014.

# A Novel Secure Encryption Scheme in MANET

A. Pratapa Reddya[#1], and Dr. N. Satyanarayana[*2]

[#]*Associate Professor, Dept. of CSE, Ganapthy Engineering College, Warangal, AP*

[1]prathapreddy54@gmail.com

**Professor, Dept. of CSE, Nagole Institute of Science& Technology, AP*

**Abstract—In a Mobile ad hoc networks (MANET) comfortable for many data transmission between any two nodes in wireless medium. Though mobile networks communication processes are carried out in effectively, some obstacles or problems in secure transmission in data. Even though there are some existing works in this area, they moreover necessitate bidirectional communications between the base station and users in each aggregation epoch, or have high-computation transparency and cannot sustain huge plaintext spaces. To address these problems, we propose an efficient secure encryption scheme for data transmission between the mobile nodes in networks. In this paper, we analyze how to organize mobile network system to diminish the energy enthusiastic by data encryption. In order to reduce energy and for secure data transmission, we propose a novel encryption scheme to provide confidentiality for network coded Mobile Ad Hoc Networks in an energy-efficient way. Through theoretical analysis and extensive simulation study show that our system outperforms other existing approaches. Our proposed techniques are effective and efficient when compared to the previous approaches through our experimental and simulation analysis.**

**Index Terms— Wireless mobile network, network security, secure data transmission, Compromised node, lightweight protocol, network coding**

## I. INTRODUCTION

Nowadays A fundamental characteristic [1] of wireless ad hoc networks is the time difference of the channel potency of the original communication links. Such time difference occur at numerous occasion scales and can be owing to multipath desertion, pathway loss using space attenuation, shadowing by obstacles, and intrusion from extra users. The impact of such time difference on the design of wireless ad hoc networks permeates throughout the layers, ranging from coding and power control at the physical layer to cellular handoff and coverage planning at the networking layer. An important means to cope with the time variation of the channel is the use of diversity. The basic design is to recover presentation by creating numerous autonomous signal ways flanked by the source and the target nodes. These diversity modes pertain to a point-to-point link. Recent results point to another form of diversity, inherent in a wireless network with multiple users. Overall system throughput is maximized by allocating at any time the common channel resource to the user that can best exploit it. Similar results can be obtained for the downlink from the base station to the mobile users.

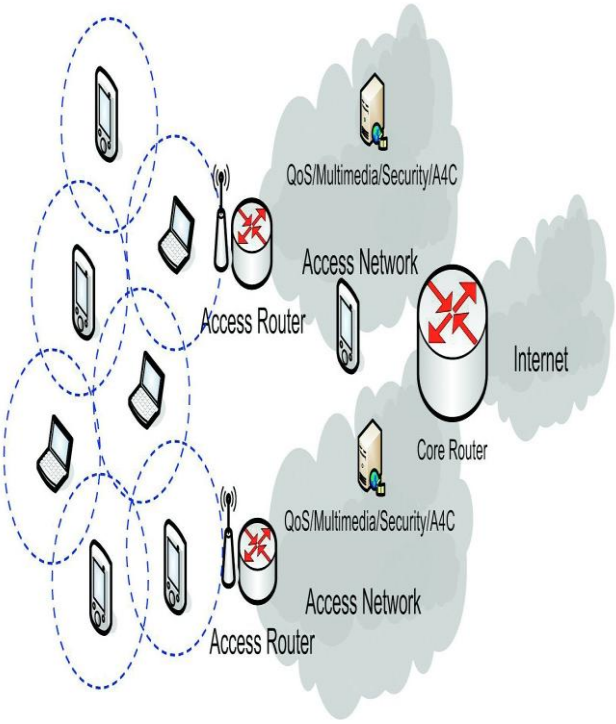



Figure 1: Network Topology for MANET

Although there are some differences between the traditional wired network and the mobile ad hoc network intrusion detection technique, which is developed first in the wired network and has become a very important security solution for the wired network, has also gained some attentions from the researchers when they explore the security solution for the mobile ad hoc network. In the following, we discuss some

typical intrusion detection techniques in the mobile ad hoc networks in details.

The unreliability of the wireless network between the two nodes happens due to the limited energy supply and the mobility of the random nodes. Due to the continuous mobility of nodes in wireless medium, the nodes can continuously move into and out of radio range of the other nodes in the ad hoc network and the routing information will be changing all the time because of the movement of the nodes. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issues so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol. These are all happens due to the network structure because there is no centralized server to control data flow or mobility of the nodes. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs. To address these problems, we propose an efficient secure encryption scheme for data transmission between the mobile nodes in networks. In this paper, we analyze how to organize mobile network system to diminish the energy enthusiastic by data encryption.

The rest of the paper will be organized as follows: In section 2, we see about the related works of the paper. In section 3, we discuss about the proposed method. The algorithms are shown in the section 4. The conclusion of our paper is in section 5.

## II. Related Works

Due to the importance of aggregation computation for WSN, secure aggregation has received great attention in recent years. And also we discuss about secure data transmission between the nodes.

As a promising [5] communication paradigm, Cognitive Radio Networks (CRNs) have paved a road for Secondary Users (SUs) to opportunistically exploit unused licensed spectrum without causing unacceptable interference to Primary Users (PUs). In this paper, we study the distributed data collection problem for asynchronous CRNs, which has not been addressed before. First, we study the Proper Carrier-sensing Range (PCR) for SUs. By working with this PCR, an SU can successfully conduct data transmission without disturbing the activities of PUs and other SUs. Subsequently, based on the PCR, we propose an Asynchronous Distributed Data Collection (ADDC) algorithm with fairness consideration for CRNs. ADDC collects data of a snapshot to the base station in a distributed manner without any time synchronization requirement. The algorithm is scalable and more practical compared with centralized and synchronized algorithms. Through comprehensive theoretical analysis, we show that ADDC is order-optimal in terms of delay and capacity, as long as an SU has a positive probability to access the spectrum. Finally, extensive simulation results indicate that ADDC can effectively finish a data collection task and significantly reduce data collection delay.

The purpose [21], [23] of a wireless sensor network (WSN) is to provide the users with access to the information of interest from data gathered by spatially distributed sensors. Generally the users require only certain aggregate functions of this distributed data. Computation of this aggregate data under the end-to-end information flow paradigm by communicating all the relevant data to a central collector node is a highly inefficient solution for this purpose. An alternative proposition is to perform in-network computation. This, however, raises questions such as: what is the optimal way to compute an aggregate function from a set of statistically correlated values stored in different nodes; what is the security of such aggregation as the results sent by a compromised or faulty node in the network can adversely affect the accuracy of the computed result. In this paper, we have presented an energy-efficient aggregation algorithm for WSNs that is secure and robust against malicious insider attack by any compromised or faulty node in the network. In contrast to the traditional snapshot aggregation approach in WSNs, a node in the proposed algorithm instead of unicasting its sensed information to its parent node, broadcasts its estimate to all its neighbors. This makes the system more fault-tolerant and increase the information availability in the network. The simulations conducted on the proposed algorithm have produced results that demonstrate its effectiveness.

Sensor networks are collection [9] [8] of sensor nodes which co-operatively send sensed data to base station. As sensor nodes are battery driven, an efficient utilization of power is essential in order to use networks for long duration hence it is needed to reduce data traffic inside sensor networks, reduce amount of data that need to send to base station. The main goal of data aggregation algorithms is to gather and aggregate data in an energy efficient manner so that network lifetime is enhanced. Wireless sensor networks (WSN) offer an increasingly Sensor nodes need less power for processing as compared to transmitting data. It is preferable to do in network processing inside network and reduce packet size. One such approach is data aggregation which attractive method of data gathering in distributed system architectures and dynamic access via wireless connectivity. Wireless sensor networks have limited computational power and limited memory and battery power, this leads to increased complexity for application developers and often results in applications that are closely coupled with network protocols. In this paper,

a data aggregation framework on wireless sensor networks is presented. The framework works as a middleware for aggregating data measured by a number of nodes within a network. The aim of the proposed work is to compare the performance of TAG in terms of energy efficiency in comparison with and without data aggregation in wireless sensor networks and to assess the suitability of the protocol in an environment where resources are limited.

Wireless Sensor Network [11] is a field of research which is viable in every application area like security services, patient care, traffic regulations, habitat monitoring and so on. The resource limitation of small sized tiny nodes has always been an issue in wireless sensor networks. Various techniques for improving network lifetime have been proposed in the past. Now the attention has been shifted towards heterogeneous networks rather than having homogeneous sensor nodes in a network. The concept of partial mobility has also been suggested for network longevity. In all the major proposals; clustering and data aggregation in heterogeneous networks has played an integral role. This paper contributes towards a new concept of clustering and data filtering in wireless sensor networks. In this paper we have compared voronoi based ant systems with standard LEACH-C algorithm and MTWSW with TWSW algorithm. Both the techniques have been applied in heterogeneous wireless sensor networks. This approach is applicable both for critical as well as for non-critical applications in wireless sensor networks. Both the approaches presented in this paper outperform LEACH-C and TWSW in terms of energy efficiency and shows promising results for future work.

Wireless Sensor Networks [15] have a wide range of applications including environmental monitoring. These networks consist of wireless sensor nodes which are densely deployed to provide a wider coverage area. The dense deployment of the sensor node provides spatial correlation in the network. In this paper an efficient data gathering approach is implemented by combining the dual prediction and clustering algorithm. Clustering algorithm based on spatial correlation is used to cluster the sensor nodes. Then within the cluster, the nodes send their data to the sink using the Normalized Least Mean Square dual prediction algorithm. Simulation results show that the proposed algorithm reduces the average energy consumption of the network.

In wireless sensor network [7], data fusion is considered an essential process for preserving sensor energy. Periodic data sampling leads to enormous collection of raw facts, the transmission of which would rapidly deplete the sensor power. In this paper, we have performed data aggregation on the basis of entropy of the sensors. The entropy is computed from the proposed local and global probability models. The models provide assistance in extracting high precision data from the sensor nodes. We have also proposed an energy efficient method for clustering the nodes in the network. Initially, sensors sensing the same category of data are placed within a distinct cluster. The remaining unclustered sensors estimate their divergence with respect to the clustered neighbors and ultimately join the least-divergent cluster. The overall performance of our proposed methods is evaluated using NS-2 simulator in terms of convergence rate, aggregation cycles, average packet drops, transmission cost and network lifetime. Finally, the simulation results establish the validity and efficiency of our approach.

Wireless sensor networks [3] [20] (WSNs) are more likely to be d-pistributed asynchronous systems. In this paper, we investigate the achievable data collection capacity of realistic distributed asynchronous WSNs. Our main contributions include five aspects. First, to avoid data transmission interference, we derive an $\Re 0$-proper carrier-sensing range ($\Re 0$-PCR) under the generalized physical interference model, where $\Re 0$ is the satisfied threshold of data receiving rate. Taking $\Re 0$-PCR as its carrier-sensing range, any sensor node can initiate a data transmission with a guaranteed data receiving rate. Second, based on $\Re 0$-PCR, we propose a Distributed Data Collection (DDC) algorithm with fairness consideration. Theoretical analysis of DDC surprisingly shows that its achievable network capacity is order-optimal and independent of network size. Thus, DDC is scalable. Third, we discuss how to apply $\Re 0$-PCR to the distributed data aggregation problem and propose a Distributed Data Aggregation (DDA) algorithm. The delay performance of DDA is also analyzed. Fourth, to be more general, we study the delay and capacity of DDC and DDA under the Poisson node distribution model. The analysis demonstrates that DDC is also scalable and order-optimal under the Poisson distribution model. Finally, we conduct extensive simulations to validate the performance of DDC and DDA.

We Data collection [13] is a common operation of Wireless Sensor Networks (WSNs). The performance of data collection can be measured by its achievable network capacity. Most of the current works on the network capacity issue are based on the deterministic network model, which is not practical for real applications due to the “transitional region phenomenon” [22]. The probabilistic network model is actually a more practical one. In this paper, we investigate the achievable Snapshot/Continuous Data Collection (SDC/CDC) capacity for WSNs under the probabilistic network model. For SDC, we propose a novel Cell-based Multi-Path Scheduling (CMPS) algorithm, whose achievable network capacity is $\Omega(po/3\omega \cdot W)$ in the worst case and $\Omega(po/\omega \cdot W)$ in the average case, where po is the promising transmission threshold probability, $\omega$ is a constant, and W is the data transmitting rate over a wireless channel, i.e. the channel bandwidth, which are both order-optimal. For CDC, we propose a Zone-based Pipeline Scheduling (ZPS) algorithm. ZPS significantly speeds up the

data collection process and achieves surprising network capacities for both the worst case and the average case. The simulation results also validate that the proposed algorithms significantly improve network capacity compared with the existing works.

Yih-Chun Hu, Adrian Perrig and David B. Johnson [4], as mobile ad hoc network applications are deployed; security emerges as a central requirement. In this paper we introduce the wormhole attack, a severe attack in ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. For example, most existing ad hoc network routing protocols, without some mechanism to defend against the wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication. We present a new, general mechanism, called packet leashes, for detecting and thus defending against wormhole attacks, and we present a specific protocol, called TIK, that implements leashes.

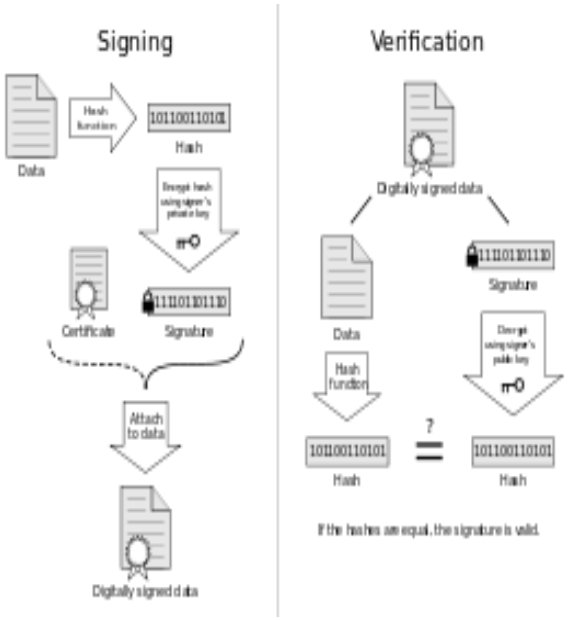
## III. Proposed System

Recently, wireless ad hoc networks are used in diverse environments to acquire different tasks such as investigate adversity relief, particular object or target tracking and also a number of tasks in elegant environments. We propose an efficient protocol for encryption and key verification in wireless network for secure data transmission. We propose an effective verification system for works against attacks in compromised nodes in the network topology. By proposing this method, we achieve Node Deployment, Broadcasting effectively, making node's sensing data operation, Effective path finding and to reduce energy consumption.

In a MANET, our network coding proposed for combines symbols of every oblique packets or information (packet prefixed with its coding vector) using encryption and key generation, to create it hard for attacker to situate coding vectors for packet or information decoding. We show that network coding is inherently weakly-secure with high probability, when the coding vectors are randomly chosen over a large finite field. In this paper, we analyze how to organize mobile network system to diminish the energy enthusiastic by data encryption. In order to reduce energy and for secure data transmission, we propose a novel encryption scheme to provide confidentiality for network coded Mobile Ad Hoc Networks in an energy-efficient way. Our proposed techniques are effective and efficient when compared to the previous approaches through our experimental and simulation analysis.

## IV. Algorithm

A Key generation and verification for our proposed encryption scheme in this paper, is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.




### A. *Generation Phase:*

Let $H$ be the hashing function and $m$ the message:
Generate a random per-message value $k$ where $0 < k < q$
Calculate $r = \left(g^k \bmod p\right) \bmod q$
In the unlikely case that $r = 0$, start again with a different random $k$
Calculate $s = k^{-1}\left(H\left(m\right) + xr\right) \bmod q$
In the unlikely case that $s = 0$, start again with a different random $k$
The signature is $(r, s)$

The first two steps amount to creating a new per-message key. The modular exponentiation here is the most computationally expensive part of the signing operation, and it may be computed before the message hash is known. The modular inverse $k^{-1} \bmod q$ is the second most expensive part, and it may also be computed before the message hash is known.

*B. Verification Phase:*

Reject the signature if $0 < r < q$ or $0 < s < q$ is not satisfied.

Calculate $w = s^{-1} \bmod q$

Calculate $u_1 = H(m) \cdot w \bmod q$

Calculate $u_2 = r \cdot w \bmod q$

Calculate $v = ((g^{u_1} y^{u_2}) \bmod p) \bmod q$

The signature is valid if $v = r$

The signature scheme is correct in the sense that the verifier will always accept genuine signatures. This can be shown as follows:

First, if g = h(p − 1)/q mod p it follows that gq ≡ hp − 1 ≡ 1 (mod p) by Fermat's little theorem. Since g > 1 and q is prime, g must have order q.

The signer computes

$$s = k^{-1}(H(m) + xr) \bmod q$$

Thus

$$\begin{aligned} k &\equiv H(m)s^{-1} + xrs^{-1} \\ &\equiv H(m)w + xrw \pmod q \end{aligned}$$

Since g has order q (mod p) we have

$$\begin{aligned} g^k &\equiv g^{H(m)w} g^{xrw} \\ &\equiv g^{H(m)w} y^{rw} \\ &\equiv g^{u1} y^{u2} \pmod p \end{aligned}$$

Finally, the correctness of DSA follows from

$$\begin{aligned} r &= (g^k \bmod p) \bmod q \\ &= (g^{u1} y^{u2} \bmod p) \bmod q \\ &= v \end{aligned}$$

## V. Conclusion

We briefly initiate the basic uniqueness of the mobile ad hoc network. Because of the appearance of the thought persistent computing, there is an increasing necessitate for the complex users to get association with the world anytime at anywhere, which encourage the appearance of the mobile ad hoc network. However, with the expediency that the mobile ad hoc networks have convey to us, there are also escalating security intimidation for the mobile ad hoc network, which necessitate to expand adequate consideration. We then discuss some typical and dangerous vulnerabilities in the mobile ad hoc networks, most of which are caused by the characteristics of the mobile ad hoc networks such as mobility, constantly changing topology, open media and limited battery power. To address these problems, we proposed a competent protected encryption scheme for information communication between the mobile nodes in networks. In this paper, we analysed to diminish the energy enthusiastic by data encryption with the help of key generation and verification protocols. Through theoretical analysis and extensive simulation study show that our system outperforms other existing approaches. Our proposed techniques are effective and efficient when compared to the previous approaches through our experimental and simulation analysis.

## References

[1] T.X. Brown, J.E. James, and A. Sethi, "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130, 2006.

[2] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-Based Anti-Jamming Techniques in Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan. 2007.

[3] A. Chan, X. Liu, G. Noubir, and B. Thapa, "Control Channel Jamming: Resilience and Identification of Traitors," Proc. IEEE Int'l Symp. Information Theory (ISIT), 2007.

[4] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper, "Intelligent Sensing and Classification in Ad Hoc Networks: A Case Study," IEEE Aerospace and Electronic Systems Magazine, vol. 24, no. 8, pp. 23-30, Aug. 2009.

[5] Y. Desmedt, "Broadcast Anti-Jamming Systems," Computer Networks, vol. 35, nos. 2/3, pp. 223-236, Feb. 2001.

[6] K. Gaj and P. Chodowiec, "FPGA and ASIC Implementations of AES," Cryptographic Engineering, pp. 235-294, Springer, 2009.

[7] O. Goldreich, Foundations of Cryptography: Basic Applications. Cambridge Univ. Press, 2004.

[8] B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall, "Improving Wireless Privacy with an Identifier-Free Link Layer Protocol," Proc. Int'l Conf. Mobile Systems, Applications, and Services (MobiSys), 2008.

[9] IEEE, IEEE 802.11 Standard, http://standards.ieee.org/getieee802/download/802.11-2007.pdf, 2007.

[10] A. Juels and J. Brainard, "Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks," Proc. Network and Distributed System Security Symp. (NDSS), pp. 151-165, 1999.

[11] M. Cetin, L. Chen, J. Fisher, A. Ihler III, M. Wainwright, and A. Willsky, "Distributed Fusion in Sensor Networks," IEEE Signal Processing Magazine, vol. 23, no. 4, pp. 42-55, Dec. 2006.

[12] A.H. Sayed, A. Tarighat, and N. Khajehnouri, "Network-Based Wireless Location: Challenges Faced in Developing Techniques for Accurate Wireless Location Information," IEEE Signal Processing Magazine, vol. 22, no. 4, pp. 24-40, July 2005.

[13] N. Patwari, J.N. Ash, S. Kyperountas, A. Hero, R.L. Moses, and N.S. Correal, "Locating the Nodes: Cooperative Localization in Wireless Sensor Networks," IEEE Signal Processing Magazine, vol. 22, no. 4, pp. 54-69, July 2005.

[14] P.H. Tseng, K.T. Feng, Y.C. Lin, and C.L. Chen, "Wireless Location Tracking Algorithms for Environments with Insufficient Signal Sources," IEEE Trans. Mobile Computing, vol. 8, no. 12, pp. 1676-1689, Dec. 2009.

[15] T. Li, A. Ekpenyong, and Y.F. Huang, "Source Localization and Tracking Using Distributed Asynchronous Sensors," IEEE Trans. Signal Processing, vol. 54, no. 10, pp. 3991-4003, Oct. 2006.
[16] L. Mihaylova, D. Angelova, D.R. Bull, and N. Canagarajah, "Localization of Mobile Nodes in Wireless Networks with Correlated in Tim Measurement Noise," IEEE Trans. Mobile Computing, vol. 10, no. 1, pp. 44-53, Jan. 2011.
[17] Y. Zou and K. Chakrabarty, "Distributed Mobility Management for Target Tracking in Mobile Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 8, pp. 872-887, Aug. 2007.
[18] R. Rao and G. Kesidis, "Purposeful Mobility for Relaying and Surveillance in Mobile Ad Hoc Sensor Networks," IEEE Trans. Mobile Computing, vol. 3, no. 3, pp. 225-231, Mar. 2004.
[19] C.D. Yang and C.C. Yang, "A Unified Approach to Proportional Navigation," IEEE Trans. Aerospace and Electronic Systems, vol. 33, no. 2, pp. 557-567, Apr. 1997.
[20] M. Mehrandezh, M.N Sela, R.G Fenton, and B. Benhabib, "Proportional Navigation Guidance for Robotic Interception of Moving Objects," J. Robotic Systems, vol. 17, no. 6, pp. 321-340, 2000.

A Pratapa Reddy obtained his Bachelor of Technology degree in Mechanical Engineering from Kakatiya University, Warangal, A.P. Then he obtained his Master of Technology degree in Computer Science & Engineering from JNTUH, Hyderabad, A.P. and pursuing PhD in Computer Science & Engineering from JNTUH, Hyderabad, A.P. Currently, he is a Assoc. Prof. at the Department of Computer Science and Engineering, Ganapathy Engineering College, Warangal, A.P. His specializations include networking, MANET, Network Security. His current research interests are wireless communications and networking, MANET, Network Security.

Dr.N.Satyanarayana, M.Sc, M.Phil, AMIE(ET), M.Tech (CS), Ph.D (CSE), MISTE,MCSI, received his Ph.D degree in Computer Science & Engineering from Acharya Nagarjuna University, currently working as a Professor in department of CSE at Nagole Institute Of Science & technology. His research interests include Advanced Computer Architecture, Networking, and Wireless Communications.