INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A SPECIAL INTRUSION-DETECTION SYSTEM FOR MANETS

Syeda Chand Sultana[1], Prof, K. Sreenivasulu[2](Ph.D.)

[1]M.Tech Student Department of CSE, Madina Engineering College, Kadapa, Andhra Pradesh, India[1],
Email :s.sundulu@gmail.com[1]
[2]Prof, Head of Department of CSE, Madina Engineering College, Kadapa, Andhra Pradesh, India[2]
Email:sreen.ukutala@gmail.com[2]

Abstract: - In past few decades the wired network technology most wide spread network in global trend. Now the technology has been migration to wireless network from wired network. In wireless networks a scalable and mobility is brought by in many applications. Among all the specifications of wireless networks, MANET is one of the most important and different applications. On the specification of traditional network architecture, actually MANET does not require a fixed network infrastructure; because the transmitter and receiver work on every single node. The communication is done in nodes within the specific range. Otherwise, they rely on their neighbours to relay messages. But the self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-special detection mechanisms described to protect MANET from attacks. With the development of the technology MANETs used into industrial applications to reach such trend, the potential security issues occur in many industrials. To deploy this situation, we propose a special implement a new intrusion-detection system named Special Enhanced Adaptive Acknowledgment (SEAACK) specially designed for MANETs. Compared to contemporary approaches, SEAACK demonstrates higher malicious-behaviour-detection rates in certain circumstances while does not greatly affect the network performances.

Keywords*:* MANET, RSA, DSA, Intrusion detection system, Secure Adaptive Acknowledgement

1. Introduction

The Wireless networking is the platform for working with the present technology used widely in many more applications. MANETs combine wireless communication with higher level mobility node [1]. But the restricted range wireless communication and higher level node mobility i.e.; the nodes of MANET must cooperate with each other to provide required networking, with the underlying of network dynamically changing to ensure so that needs are continuously met. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in serious mission applications like military conflict or emergency recovery. A nominal configuration and quick deployment make MANET ready to be used in emergency conditions where an infrastructure is unavailable or infeasible to install in scenarios like natural or military conflicts, human-induced disasters, and medical emergency situations. Owing to these unique characteristics, MANET is becoming more broadly implemented in the industry [14]. However, considering the fact that MANET is popular among critical applications, network security is of fundamental importance. Unfortunately, remote distribution of MANET and the open medium make it vulnerable to different types of attacks. For example, owing to the node's lack of physical protection, malicious attackers can easily confine and compromise nodes to achieve attacks [7].

***1.1 TWOACK*:** With respect to the six weaknesses of activities that violate the security rules. We the Watchdog scheme, many researchers proposed new has proposed novel IDS named EAACK protocol approaches to solve these issues. TWOACK proposed specially designed for MANETs and compared it against one of the most important approaches among them [7].

***1.2 Watchdog*:** Watchdog that aims to improve the path from the source to the destination. The throughput of network with the presence of malicious TWOACK scheme successfully solves the nodes. In fact, the Watchdog scheme is consisted of two receiver Collision and limited transmission power problems parts, namely, Watchdog and Path ratter. Watchdog posed by Watchdog. However, the acknowledgment serves as IDS for MANETs [13]. It is responsible for detecting process required in every packet transmission process malicious node misbehave in the network [12]. Watchdog added a significant amount of unwanted network listening to its next hop's transmission.

2. PROPOSED SYSTEM:

In proposed system we design the SEAAK with MANET, RSA, DSA, Intrusion detection.secure Adaptive Acknowledgement [1], [13].

2.1. MANET:

In many traditional mobile networking scenarios, nodes establish communication on the basis of public identities. However, in some settings, node identities must not be exposed and node movements should not be traceable. Instead, nodes need to communicate on the basis of their current locations. Such scenarios are encountered in mission critical mobile ad-hoc networks (MANETs) [2], Vehicular ad-hoc networks (VANETs) and delay-tolerant-networks (DTNs) and in the near future geo-social mobile networks [4][3]. In this project, we consider a number of issues arising in such settings by designing anonymous location based routing protocols [9]. We have designed two protocols so far: ALARM and PRISM . ALARM is a link state based protocol which uses nodes' current locations to disseminate and construct topology snapshots. PRISM is a reactive protocol based on AODV which achieves similar goals. With the aid of advanced cryptographic primitives (i.e., group signatures), both protocols provide a mix of security and privacy features, including: node authentication, data integrity, anonymity and UN traceability (tracking-resistance) [5]. ALARM also offers protection against insider attacks. Another important issue in location based MANET/VANETs is secure location verification. We propose new techniques to securely verify locations of nodes in group settings using distance bounding protocols (Group Distance Bounding). Our techniques are a generalization of the single proves single verifier distance bounding protocols. Key differences between MANETs and other wireless networks (Cellular Networks or Wireless LANs) are:

2.1.1No Fixed Routing/Forwarding Infrastructure:

Unlike the Internet or other forms of wireless networks (e.g., cellular mobile networks) MANETs don't have a fixed infrastructure that nodes can rely on for forwarding messages. This is the main reason why the design and operation of such networks is challenging. This also raises new security and privacy concerns.

2.1.2 Collaboration:

Due to the lack of forwarding infrastructure, MANET nodes have to rely on each other in forwarding traffic. This gives attackers who control MANET nodes the ability to drop packets, reroute them. Attackers can also easily impersonate other nodes and/or violate their privacy by tracking their movements [8].

2.1.3Un trusted Environment:

One of the main uses of MANETs is in mission critical networks. Such networks are used in military, law enforcement and search/rescue operations. MANETs may thus be deployed in hostile environments where adversaries will try to disrupt the operation of the network and compromise the security and privacy of the nodes.

2.1.4 No PKI and On-line Security Infrastructure:

Unlike the Internet or other forms of wireless networks most MANETs don't have a fixed on-line security infrastructure [10]. Any solution relying on on-line trusted third parties will thus be challenging to implement and operate. As shown in the figure 1 and figure 2

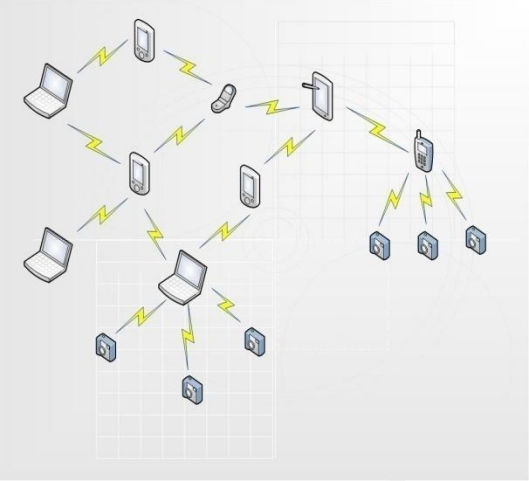


Figure 1: Wireless Network

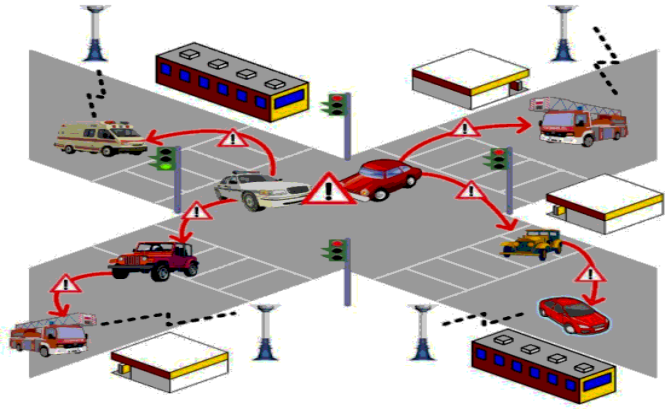


Figure 2: Traffic Control in MANET's Nodes

For Tracking Their Movements

2.2 RSA:

RSA encryption is an Algorithm understood by so few people and used by many. In hopes to help that large percentage understand RSA Encryption better I wrote this explanation. If you ever visit a https site chances are you are using RSA encryption to encrypt or scramble the data sent over the internet. Since you could be sending important information like a credit card number it is imperative that you encrypt the data. The important thing is that we want to do this encryption process without requiring secret keys that both the sender and the recipient must possess. That's where a system that uses a "Public Key" comes in handy. As shown in below figure 3.

2.2.1 Generate a public key and private key:

First we need our keys: A private key that the server will keep and a public key that can be given away.

We need 2 prime numbers:

p & q . p = 29, q = 31

Calculate n = p * q = 29 * 31 = 899

Calculate t = (p -1) * (q – 1) = (29 – 1) * (31 – 1) = 840

Choose a prime number e. e needs to be relatively prime to t (t cannot be divisible by e) Let's pick 11 we now need to find a d. We will use the formula: d * e [=] 1 mod t. This means (d * 11) / t will give us a remainder of one. You have to find the inverse of e mod t. If you're interested in how this can be computed please check my other post here. Since we are dealing with such small numbers we can sort of guess our d until we find one that works.

(611 * 11) = 6721, 6721 / 840 = 8 with remainder 1. So 611 works! We now have everything we need for a private and public key to encrypt our data.

p – 29

q – 31

n – 899

t – 840

e – 11

d – 611

Our public key becomes n and e.

Our private key becomes n and d.

2.2.2 Encrypting our message:

We give our public key numbers to the person that wants to send us their message. They will encrypt the message with the formula:

C = M mod n

C is our encrypted Message. So if we took the letter 'w' who's ASCII value is 119.

C = 119 mod 899 = 595

We now send 595 to the server.

2.2.3 Decrypting our message:

In order to decrypt the message we need our private key n and d Keep in mind we don't give anybody our private key. We use the formula M = C mod n so M = 595 mod 899 = 119 M = 119 whose character value is 'w'

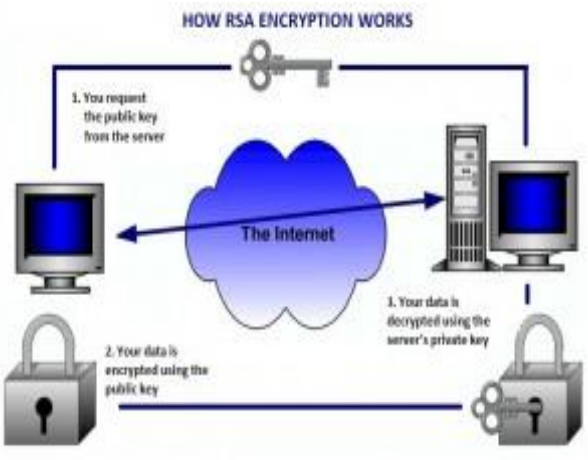


Figure 3: RSA Routing

3. RSA:

Digital signatures are essential in today's modern world to verify the sender of a document's identity. A digital signature is represented in a computer as a string of binary digits. The signature is computer using a set of rules and parameters (algorithm) such that the identity of the person signing the document as well as the originality of the data can be verified. The signature is generated by the use of a private key. A private key is known only to the user. The signature is verified makes use of a public key which corresponds to (but not the same, i.e. mathematically infeasible to deduct private key from public) the private key. With every user having a public/private key pair, this is an example of public-key cryptography. Public keys, which are known by everyone, can be used to verify the signature of a user. The private key, which is never shared, is used in signature generation, which can only be done by the user. Digital signatures are used to detect unauthorized modifications to data. As shown in figure 4, Also, the recipient of a digitally signed document in proving to a third party that the document was indeed signed by the person who it is claimed to be signed by. This is known as non-repudiation, because the person who signed the document cannot repudiate the signature at a later time. Digital signature algorithms can be used in e-mails, electronic funds transfer, electronic data interchange, software distribution, data storage, and just about any application that would need to assure the integrity and originality of data. As shown in figure 3

DSA Parameters:

- p = a prime modulus, where $2^{L-1} < p < 2^{L}$ for $512 \leq L \leq 1024$ and L is a multiple of 64. So L will be one member of the set {512, 576, 640, 704, 768, 832, 896, 960, 1024}
- q = a prime divisor of p-1, where $2^{159} < q < 2^{160}$

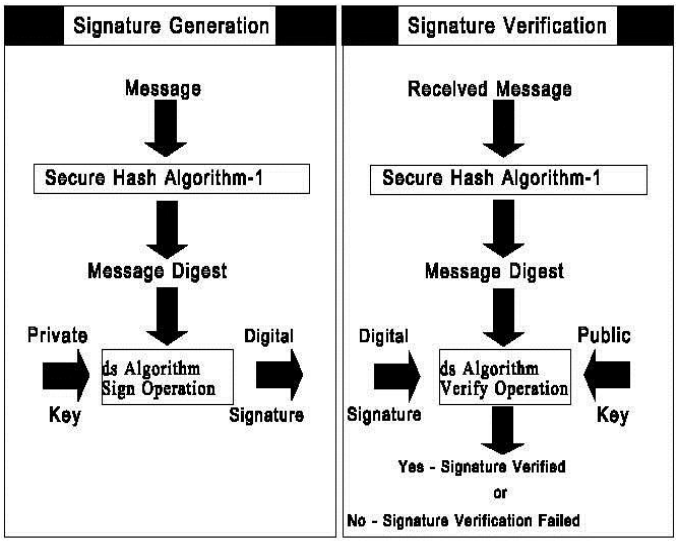


Figure 4: Message Encryption and Decryption

4. Intrusion Detection System:

Intrusion detection is very important aspect of defending the cyber infrastructure from attackers or hackers. Intrusion prevention technique such as filtering router policies and firewalls fail to stop such kind of attacks [15]. Therefore, no matter how well a system is protected, intrusion still occurs and so they should be detected. Intrusion detection systems are becoming significant part of security and the computer system. An intrusion detection system is used to detect many types of malicious behaviours of nodes that can compromise the security and trust of a computer system. To address this problem, IDS should be added to enhance the security level of MANETs. If MANET knows how to detect the attackers as soon as they enter the network, we will be able to completely remove the potential damages caused by compromised nodes at the first time. IDSs are a great complement to existing proactive approaches and they usually act as the second layer in MANETs. There is a need for IDS to implement an intelligent control mechanism in order to monitor and recognize security breach attempts efficiently over a period of the expected network lifetime [8].

5. Secure Adaptive Ack:

Based on TWOACK, we proposed a new scheme that is called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which can be measured as a combination of a scheme called TACK (identical to TWOACK) and an end-to-end acknowledgment scheme called Acknowledge (ACK). Compared to TWOACK, AACK considerably reduces network overhead while still capable of maintaining or even surpassing the same network throughput during data transmission.

The end-to-end acknowledgment scheme in ACK is shown in figure 5. The ACK scheme the source node S sends out Packet 1 without any overhead except 2 b of flag indicating the packet type. In this network all the intermediate nodes simply forward this packet to the next nodes. When the destination node D receives Packet 1, it is vital to send back an ACK acknowledgment packet to the source node S down the reverse order of the same route. Within a predefined time, if the source node S receives this ACK acknowledgment packet from the destination node, then the packet transmission from node S to node D is successful. Or else, the source node S will switch to TACK scheme by sending out a TACK packet. SEAACK—A SECURE &SPECIAL INTRUSION-DETECTION SYSTEM FOR MANETs

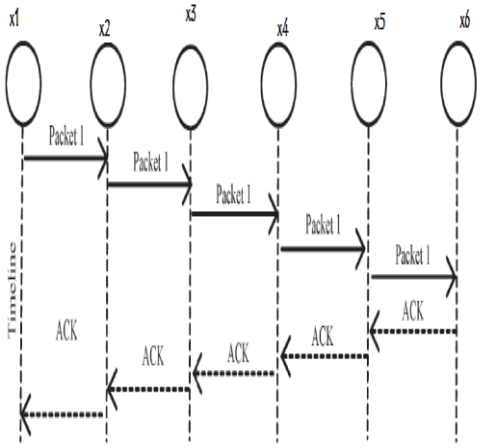


Figure 5: End-to-End ACK

6. Result Analysis:

It can be observed in Figure 6 that the packet delivery of AODV is dropped because of attacks and improved it by avoiding attackers. With the given importance to QOS, AACK improved the Packet Delivery and EDS followed AACK.

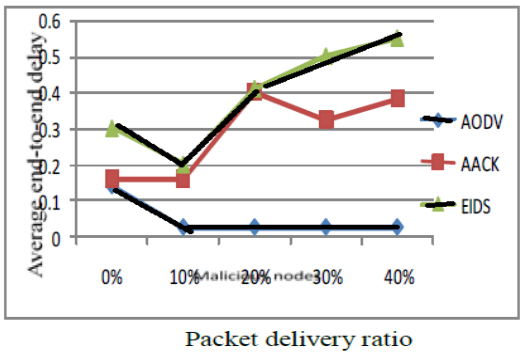
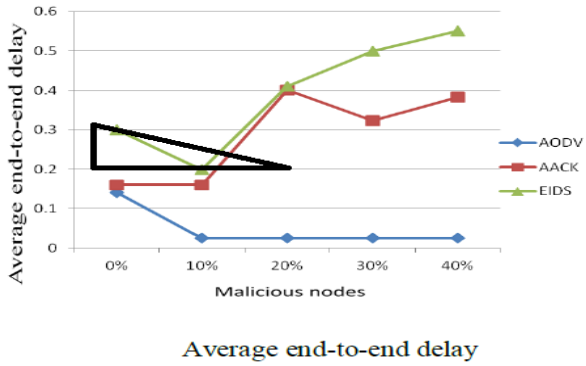


Figure 6: Packet Delivery Ratio by Using End-to-End AACK

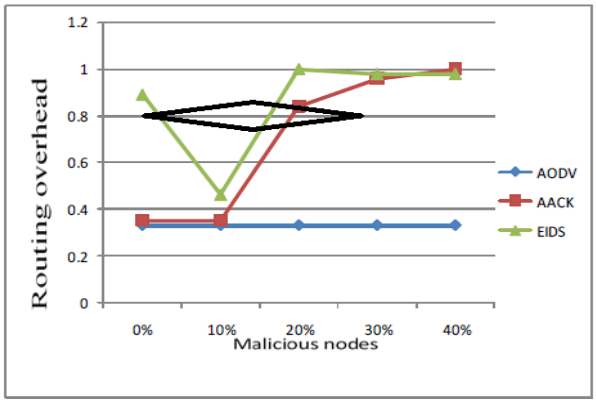
It can be observed from the below Figure 7 the end-to end caused by AODV method is more and AACK reduced it to a maximum extent up to 97.95%. EDS and AACK showed the same performance



Average end-to-end delay

Figure 7: packet delay ratio

From Figure 8 it is observed that the overhead by a little higher to AODV, AACK and EDS approximated it to AODV



Routing overhead

Figure 8: Packet overhead ratio

It is observed from the Figure 8 that as the malicious nodes count to increases, the remaining network lifetime decreases. AODV provided security, could not provide performance in terms of energy consumption. AACK provided Quality of Service, could save some energy. EDS concentrated on energy as well along with QoS, increased the network life time by 14.63% comparedto AODV and23.24% compared to SRAC.

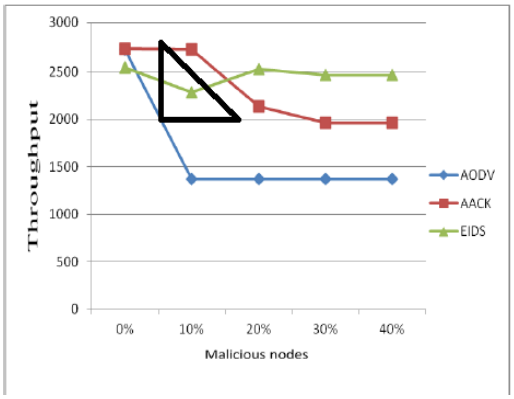


Figure 9: Detection of Malicious Nodes

7. Conclusion:

Packet-dropping attack has always been a major risk to the security in MANETs. In the present work we have proposed an Intrusion Detection System namely Improved Intrusion Detection System for MANETs and compared it against other mechanisms in different scenarios through simulations. The results demonstrated optimistic performances against AACK in the cases of receiver collision, false misbehaviour report and limited transmission power [6]. Furthermore, in an effort to prevent the attackers from initiating forged data attacks, we extended our work to incorporate security in our proposed scheme. Although it generates more Routing Overhead in the present scheme as demonstrated for some cases, it can vastly advance the network's Packet Delivery Ratio, when the attackers are smart enough to forge acknowledgment packets [11].

8. Future Enhancement:

To increase the merits of the present work, we do have plans to investigate the following issues in our future research:

- ✓ Possibilities of implementing hybrid cryptography techniques to further reduce the network overhead caused by security.
- ✓ Observe the possibilities of adopting a key exchange mechanism in order to remove the requirement of pre distributed keys.

9. REFERENCES

[1] K.Al Agha, M.-H. Bertin, T. Dang, A,Guitton, P. Minet, T. Val, and J.-B. Viollet,"Which wireless technology for industrial wireless sensor networks? The development of OCARI techno," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4266–4278, Oct. 2009.
[2] R. Albano, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.
[3] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541.
[4] T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," in Wireless/Mobile Security. New York: Springer-Verlag, 2008.
[5] L. Buttyan and J. P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.
[6] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Bernini, "Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 7, pp. 2759–2766, Jul. 2008.
[7] V. C. Gung or and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approach," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.
[8] Y. Hue, D. Johnson, and A. Per rig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proc. 4th IEEEWorkshop Mobile Compute. Syst. Appl., 2002, pp. 3 13.
[9] Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in Proc. 8th ACM Int. Conf. MobiCom, Atlanta, GA, 2002, pp. 12–23.
[10] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," J. Compute. Sci., vol. 3, no. 8, pp. 574–582, 2007.
[11] D. Johnson and D. Maltz, "Dynamic Source Routing in ad hoc wireless networks," in Mobile Computing. Norwell, MA: Kluwer, 1996, chap. 5,pp. 153–181.
[12] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodes in MANETs," in Proc. 12th Int. Conf. iiWAS, Paris, France, Nov. 8–10, 2010, pp. 216–222.
[13] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in Proc. IEEE 25th Int. Conf. AINA, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.
[14] K. Kuladinith, A. S. Timm-Giel, and C. Gorge, "Mobile ad-hoc communications in AEC industry," J. Inf. Technol. Const., vol. 9, pp. 313–323, 2004.
[15] J.-S. Lee, "A Petri net design of command filters for semiautonomous mobile sensor networks," IEEE Trans. Ind. Electron., vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

10. Biography

Syeda Chand Sultana is a student in Master of Technology in the Department of Computer Science and Engineering, Madina Engineering College, Kadapa, Andhra Pradesh, India.

K.Sreenivasulu [Ph.D], is a Professor, Head Of Department of Computer Science and Engineering, Madina Engineering College, Kadapa, Andhra Pradesh, India.