PROFICIENT AND SECLUDE DATA COMMUNICATIONONCLUSTER BASED NETWORKS

Mrs.Valivati Krishna priya,student of M.tech,depat.of CSE in Lingayas Institute Of Management And Technology.

Under Guidance of Assoc.Prof. K.Bhagavan department of CSE in Lingayas Institute Of Management And Technology

Abstract—
In Proficient and seclude data communication on Network based networks are used to wireless sensor networks .Networking is an effective and practical way to increase the system performance of WSNs is the data communication on Network based networks used recent days . In this paper, we study a Proficient and seclude data communication on Network based networks used by WSNs (CWSNs), these are in the group of itemsests called Networks are formed at the time of data transmission for each communication and periodically. Here we used AODV(Ad hoc On-Demand Distance Vector (AODV) Routing protocol which findout the shortest path and reliable path at time of data transmission.We propose Proficient and seclude data communication on Network based networkscontrol protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) protocol and the Identity-Based Offline/Online digital Signature (IBOOS) protocol, respectively. In SET-IBS, for solve the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discretemathematical logarithm problem. reduce the security overhead calculations and energy consumption.We show the feasibility of the SET-IBS and SET-IBOOS protocols to provide the security requirements and security analysis on various different attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The results show that, the proposed protocols have better performance than the existing secure protocols for CWSNs.these paper are used to show the results by NS2 tool..

Index Terms:*Network-based WSNs, ID-based digital signature, ID-based offline/online digital signature, secure data transmission protocol,Ad-hoc network,NS2 TOOL.*

I.INTRODUCTION

Proficient and seclude data communication WIRELESS sensor network (WSN) is a network system comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion. The individual nodes are capable of sensing their environments, processing the information data locally, and sending data to one or more collection points in a WSN [1]. Meanwhile, many WSNs are deployed in harsh, neglected, and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings [2]. Efficient data communication is one of the most important thing for WSNs. Secure and efficient data transmission (SET) is, thus, especially necessary and is demanded in many such practical WSNs.

II.AODV Protocol Overview

The AODV [11, 12] routing protocol is a reactive routing protocol; therefore, routes are determined only when needed. Figure 1 shows the message exchanges of theAODV protocol. Hello messages may be used to detect and monitor links to eighbors. If Hello messages are used, each active node periodically broadcasts a Hello message that all its neighbors receive. Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbor, a link break is detected.
When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination.
At each intermediate node, when a RREQ is received a route to the source is created. If the receiving node has not received this RREQ before, is not the destination and does not have a current route to the destination, it rebroadcasts

the RREQ. If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP). The RREP is unicast in a hop-byhop fashion to the source. As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it records the route to the destination and can begin sending data.

1.1 Environment And Enthusiasm

Network-based data Networks in WSNs, has been investigated by researchers in order to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes. In a -based WSN (CWSN), every Network has a leader sensor node, regarded as Network-head (CH). A CH aggregates the data collected by the leaf nodes (non- CH sensor nodes) in its Network, and sends the aggregation to the base station (BS). The LEACH (Low-Energy Adaptive Networking Hierarchy) protocol presented by Heinzelman*et al*. is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. In order to prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensor nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime. Following the idea of LEACH, a number of protocols have been presented such as APTEEN and PEACH, which use similar concepts of LEACH. In this paper, for convenience, we call this sort of Network-based protocols as LEACH-like protocols. Researchers have been widely studying CWSNs in the last decade in the literature, however, the implementation of the Network-based architecture in the real world is rather complicated.

Adding security to LEACH-like protocols is challenging, because they dynamically, randomly and periodically rearrange the network's Networks and data links. Therefore, providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols (most existing solutions are provided for distributed WSNs, but not for CWSNs). There are some secure data transmission protocols based on LEACH-like protocols, such as SecLEACH, GS-LEACH and RLEACH . Most of them, however, apply the symmetric key management for security, which suffers from a so-called orphan node problem. This problem occurs when a node does not share a pairwise key with others in its preloaded key ring, in order to mitigate the storage cost of symmetric keys, and the key ring is not sufficient for the node to share pairwise symmetric keys with all of the nodes in a network. In such a case, it cannot participate in any Network, and therefore, has to elect itself as a CH. Furthermore, the orphan node problem reduces the possibility of a node joining a CH, when the number of alive nodes owning pairwise keys decreases after a longterm operation of the network. Since the more CHs elected by themselves, the more overall energy consumed of the network, the orphan node problem increases the overhead of transmission and system energy consumption by raising the number of CHs. Even in the case that a sensor node does share a pairwise key with a distant CH but not a nearby CH, it requires comparatively high energy to transmit data to the distant CH.

The feasibility of the asymmetric key management has been shown in WSNs recently, which compensates the shortage from applying the symmetric key management for security. Digital signature is one of the most critical security services offered by cryptography in asymmetric key management systems, where the binding between the public key and the identification of the signer is obtained via a digital certificate. The Identity-Based digital Signature (IBS) scheme, based on the difficulty of factoring integers from Identity- Based Cryptography (IBC), is to derive an entity's public key from its identity

information, e.g., from its name or ID number. Recently, the concept of IBS has been developed as a key management in WSNs for security. Carman first combined the benefits of IBS and key pre-distribution set into WSNs, and some papers appeared in recent years, e.g.. The IBOOS scheme has been proposed in order to reduce the computation and storage costs of signature processing. A general method for constructing online/offline signature schemes was introduced by Even et al. The IBOOS scheme could be effective for the key management in WSNs. Specifically, the offline phase can be executed on a sensor node or at the BS prior to communication, while the online phase is to be executed during communication. Some IBOOS schemes are designed for WSNs afterwards, such as and this system. The offline signature in these schemes, however, is pre-computed by a third party and lacks reusability, thus they are not suitable for CWSNs.

hand-outs and association

Recently, we have applied and evaluated the key management of IBS to routing in CWSNs. In this paper, we extend our previous work and focus on providing efficient secure data communication for CWSNs. The contributions of this work are as follows.

• We propose two Proficient and seclude data communication on Network based networks protocols for AODV Protocols and CWSNs, called **SET-IBS** and **SETIBOOS**, by using the **IBS** scheme and the **IBOOS** scheme, respectively. The key idea of both SET-IBS and SET-IBOOS is to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security. In the proposed protocols, secret keys and pairing parameters are distributed and preloaded in all sensor nodes by the BS initially, which overcomes the key escrow problem described in ID-based crypto-systems. Full secured data storage through sensor networks.

• Secure statement in SET-IBS relies on the ID-based cryptography, in which, user public keys are their ID information. Thus, users can obtain the corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy.

• SET-IBOOS is proposed in order to further reduce the computational overhead for security using the IBOOS scheme, in which security relies on the hardness of the discrete logarithmic problem. Both SET-IBS and SETIBOOS solve the orphan node problem in the secure data transmission with a symmetric key management.

AODV PROTOCOL protocols to also the routing protocols these are the used to the process of this paper are full secured and particular process of the sensor networks.

• We show the feasibility of the proposed protocols with respect to the security requirements and analysis against three attack models. Moreover, we compare the proposed protocols with the existing secure protocols for efficiency by calculations and simulations respectively, with respect to both computation and communication.

III.SYSTEM DESCRIPTION AND PROTOCOL OBJECTIVES

This sector explained the network architecture, securityvulnerabilities, and protocol themes..

Network ArchitectureConsider a CWSN consisting of a fixed BS,AODV and a large number of wireless elements .

The BS is a trusted authority (TA).Meanwhile, the sensor nodes may be compromised byattackers, and the data transmission may be interruptedfrom attacks on wireless channel. In a CWSN, sensor nodesare grouped into clusters, and each cluster has a CH sensornode, which is elected autonomously. Leaf (non-CH) sensornodes join a cluster depending on the receiving signalstrength and transmit the sensed data to the BS via CHs tosave energy. The CHs perform data fusion, and transmitdata to the BS directly with comparatively high energy. Inaddition, we assume that all sensor nodes and the BS aretime synchronized

with symmetric radio channels, nodesare distributed randomly, and their energy is constrained. The CWSNs in data sensing, processing, and transmission consume energy of sensor elements. The cost of datatransmission is much more expensive than that of dataprocessing. Thus, the method that the intermediate node(e.g., a CH) aggregates data and sends it to the BS ispreferred than the method that each sensor node directlysends data to the BS [1], [3]. A sensor node switches intosleep mode for energy saving when it does not sense ortransmit data, depending on the time-division multipleaccess (TDMA) control used for data transmission. In thispaper, the proposed SET-IBS and SET-IBOOS are bothdesigned for the same scenarios of CWSNs above. These are all the sensors networks are used to routing protocols used by transmitted by the signal through wireless networks signals transferred by the data using protocols.

The AODV protocol message exchanges of theAODV protocol. Hello messages may be used to detect and monitor links to neighbors. If Hello messages are used, each active node periodically broadcasts a Hello message that all its neighbors receive. Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbor, a link break is detected.

When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination to the routing protocol process through sensor networks.

IV.OVERVIEW OF NS2 TOOL

Developed by UC BerkeleyMaintained by USCPopular simulator in scientific environmentOther popular network simulators and

Glomosim: UCLA, CMU; ParseC, Mobile Simulation mostly

OPNET: commercial software, graphical interface, not free;

Others: commercial ones, not free, e.g. IBM TPNS

NS2 GOALS:

• To support networking research and education

– Protocol design, traffic studies, etc.

– Protocol comparison;

– New architecture designs are also supported.

• To provide collaborative environment

– Freely distributed, open source;

– Increase confidence in result.

The NS2 tool used by the Used to build the network structure and topologywhich is just the surface of your simulatoion;Easily to configure your network parameters; protocol scheme and architecture .

NS2 TOOL WORKING:

Most important and kernel part of the NS2 implement the kernel of the architecture of rom the packet flow view, the processes run change or “comment out” the existing protoetails of your research scheme.

2 requirements of the simulator

– Detailed simulation of Protocol: Run-time speed;

– Varying parameters or configuration: easy to use. run but slower to code and change;

OTcl is easy to code but runs slowly.

MODEL OF PROTOCOL IN NS2 TOOL:

Wired Networking

– Routing: Unicast, Multicast, and Hierarchical Routing, etc.

– Transportation: TCP, UDP, others;

– Traffic sources: web, ftp, telnet, cbr, etc.

– Queuing disciplines: drop-tail, RED, etc.

– QoS: IntServ and Diffserv Wireless Networking Ad hoc routing and mobile IPSensor Networks(hmmm)

– SensorSim: built up on NS2, additional features, for TinyOS

Traffic models and applications:

Web, FTP, telnet, constant-bit rate(CBR)

Transport protocols:

Unicast: TCP (Reno,Vegas), UDP Multicast

Routing and queuing:

Wired routing, Ad Hoc routing.

Queuing protocols:

RED(Random Early Drop), drop-tail

Physical media:

Wired (point-to-point, LANs), wireless, satellite

RESEARCH BASED NS2 TOOL:

- Intserv/Diffserv (QoS)
- Multicast: Routing, Reliable multicast
- Transport: TCP Congestion control
- Application: Web caching Multimedia
- Sensor Networks: LEACH, Directed Diffusion, etc. Most are routing protocols.

STRUCTURE OF DIRECTORY IN NS2 TOOL

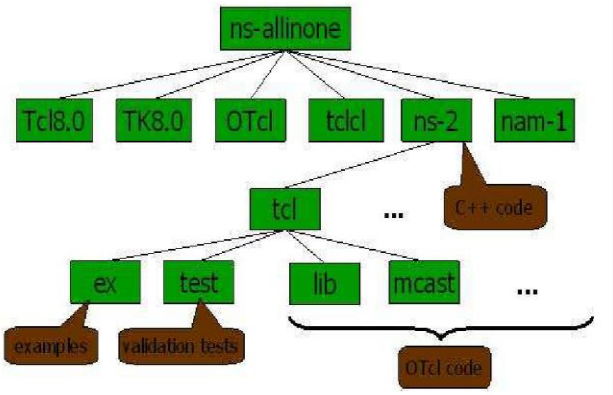


FIG. directory structure of NS2 TOOL.

These ns2 tool are used by the program are object oriented programming through the networking process are topology working is

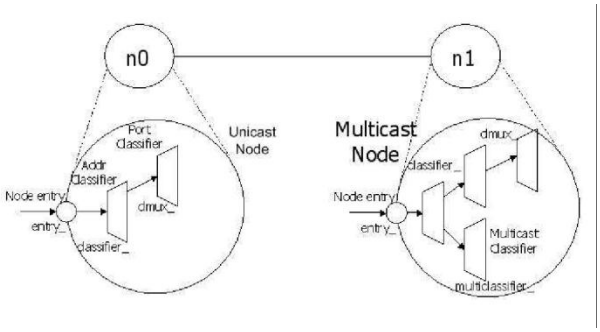


Fig. Network topology

V. Security liabilities and Protocol purpose

The data transmission protocols for WSNs, includingcluster-based protocols (LEACH-like protocols), are vulnerable to a number of security attacks [2], [23]. Especiallyattacks to CHs in CWSNs could result in serious damage tothe network because data transmission and data aggregation depend on the CHs fundamentally. If an attackemanages to compromise or pretend to be a CH, it canprovoke attacks such as sinkhole and selective forwardingattacks, hence disrupting the network. On the other handan attacker may intend to inject bogus sensing data into the WSN, for example, pretend as a leaf node sending boguinformation toward the CHs. Nevertheless, LEACH-likprotocols are more robust against insider attacks than other types of protocols in WSNs [23]. It is because CHs are rotating from nodes to nodes in the network by roundswhich makes it harder for intruders to identify the routingelements as the intermediary nodes and attack them. The characteristics of LEACH-like protocols reduce the risks of being attacked on intermediary nodes, and make it hardefor an adversary to identify and compromise important nodes (i.e., CH nodes).

VI.THE PROPOSED SET-IBS PROTOCOL and AODV PROTOCOL

In that paper process is ,the message exchanges of theAODV protocol. Hello messages may be used to detect and monitor links to eighbors. If Hello messages are used, each active node periodically broadcasts a Hello message that all its neighbors receive. Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbor, a link break is detected.
When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination.
we propose two novel SET protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the IBSscheme and the IBOOS scheme, respectively. We firstpresent SET-IBS in this section. The proposed SET-IBS has a protocol initialization priorto the network deployment and operates in rounds duringcommunication, which consists of a setup phase and a steady-state phase in each round. We introduce the protocol initialization, describe the key management of the protocol by using the IBS scheme, and the protocol operations afterwards.

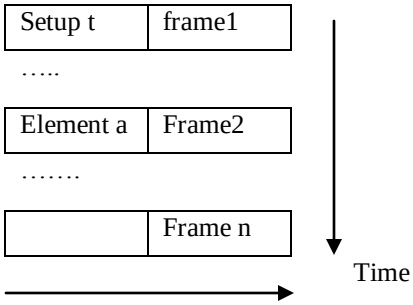


Fig. secured data communication

The sensor node is the process os secured data transmission using protocols.

$$T(n) = \frac{\rho}{1-\rho \times \left(r \bmod \left\lfloor \frac{1}{\rho} \right\rfloor\right)} \cdot \frac{E_{cur}(n)}{E_{init}(n)} \quad \forall n \in G_n, \qquad (5)$$

$$T(n) = 0 \quad \forall n \notin G_n.$$

Setup-phase:

Step1 : A1->G1 // broad to all nodes//

Step2 : B1->G1// their information//

Step3 :C1->B1//cluster of B1.//

AODV PROTOCOL MESSAGING

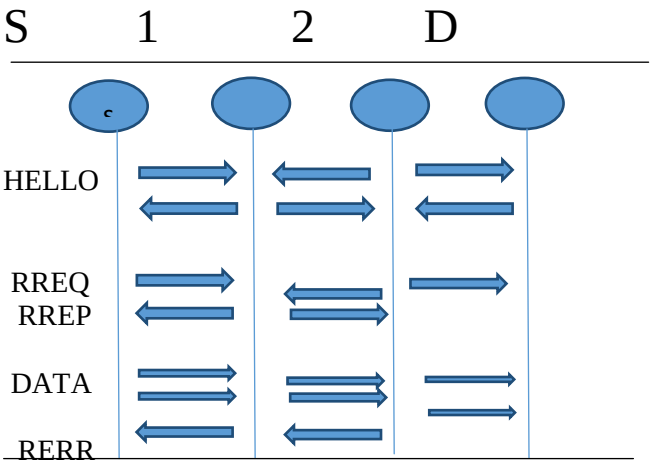


Figure 1. AODV protocol Messaging

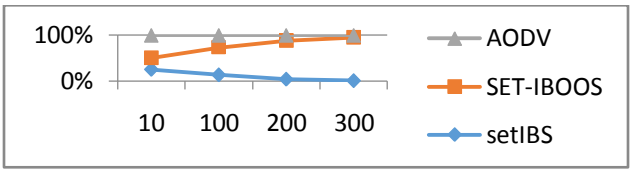
VII.PROTOCOL ATTRIBUTES

The protocol characteristics and hierarchical clusteringsolutions are presented in this section. We first summarize the features of the proposed SET-IBS,SET-IBOOS and AODV protocols as follows: .Both the proposed SET-IBS,AODV and SET-IBOOS proto-cols provide secure data transmission for CWSNswith concrete ID-based settings, which use IDinformation and digital signature for authentication. Thus, both SET-IBS, SET-IBOOS And AODV fully solve the orphan-node problem from using the symmetric key management for CWSNs..The proposed secure data transmission protocolsare with concrete ID-based settings, which use IDinformation and digital signature for verification the sensor networks.

Message Size of Data Transmission

In this part, we do the quantitative calculation of the message packet size on data transmission in the steady state(main phase) of the different protocols for comparison. Inthe proposed SET-IBS, the message packet size on transmission for node j is described in Section 4, which equals to

$$|\mathbb{D}_i| + |\mathbb{D}_j| + |t_j| + |C_j| + |\sigma_j| + |c_j|.$$

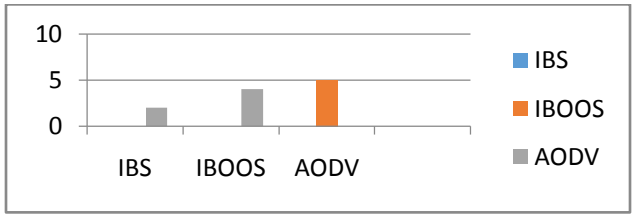


SENSOR NODES

Simulation Results

Comprehending the extra energy consumption by theauxiliary security overhead and prolonging the networklifetime are essential in the proposed SET-IBS and SET- IBOOS. To evaluate the energy consumption of the computational overhead for security in communication, we consider three metrics for the performance evaluation: Network lifetime, system energy consumption, and the number of alive nodes. For the performance evaluation, we compare theproposed SET-IBS and SET-IBOOS with LEACH protocol[4] and SecLEACH protocol [8]:.Network lifetime (the time of FND)—We use the most general metric in this paper, the time of first node dies (FND), which indicates the duration that thesensor network is fully functional [1].

Therefore,maximizing the time of FND in a WSN means toprolong the network lifetime.. The number of alive nodes—The ability of sensing and collecting information in a WSN depends on the set ofalive nodes (nodes that have not failed). Therefore,we evaluate the functionality of the WSN dependingon counting the number of alive nodes in the network.on counting the number of alive nodes in the network.. Total system energy consumption—It refers to theamount of energy consumed in a WSN. We evaluate the variation of energy consumption in secure data transmission protocols. In the network simulation experiments, 100 nodes areRandomly distributed in a 100 m Â 100 m area, with a fixedS located near part of the area, as shown in the figure ine Appendix. All the sensor nodes periodically sensevents and transmit the data packet to the BS. We assume



Protocols of communication

VIII.CONCLUTION:

In this paper, we first reviewed The Proficient And Seclude Data Communication On Network Based Networks through data transmission issues and the security issues in CWSNs. The deficiency of the symmetric key management for secure data transmission has been discussed. We then presented two secure and efficient data transmission protocols respectively for CWSNs, SET-IBS and SET-IBOOS. In the evaluation section, we provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. SET-IBS,AODV and SET-IBOOS protocols are efficient in communication and applying the ID-based crypto-system, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management. Lastly, the comparison in the calculation and simulation results show that, the proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs. With respect to both computation and communication costs, we pointed out the merits that, using SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs and these are in the used NS2 TOOL for see the result of this paper .using linux operating system.

REFERENCE

[1] The base paper referred to" Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks" Huang Lu, Student Member, IEEE, Jie Li, Senior Member, IEEE, and Mohsen Guizani, Fellow, IEEE.

[2] T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence,

[3] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Comm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.

[4] A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/15, pp. 2826-2841, 2007.

[5] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660-670, Oct. 2002.

[6] A. Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," IEEE Trans. Parallel & Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.

[7] S. Yi et al., "PEACH: Power-Efficient and Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/15, pp. 2842-2852, 2007.

[8] K. Pradeepa, W.R. Anne, and S. Duraisamy, "Design

[9] Implementation Issues of Clustering in Wireless Sensor Networks," Int'l J. Computer Applications, vol. 47, no. 11, pp. 23-28,2012.

[10] L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2007.

[11]. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks," Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA), pp. 145-152, 2007.

BIOGRAPHIE

Valiveti Krishna Priya pursuing M.Tech inLingayas institute of Management and Technology in the stream of Computer Science and Engineering and she received Master of computer Science in AcharayaNagarjunaUniverityfrom Vikas PG College in 2008. She born on 12/07/1984.