ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

Secure Data Aggregation in Wireless Sensor Network using BECAN Scheme

Miss. Priyanka G. Padmane[1], Prof. K.G. Bagde[2]

Department of Computer Science & Information Technology, Amravati University, Maharashtra, India[1]

Department of Computer Science & Engineering, Amravati University, Maharashtra, India[2]

Abstract: Wireless Sensor Networks (WSNs) are used in many applications in the area of tracking and monitoring. WSNs have many constraints like low computational power, small memory, and limited energy resources. Most of the energy consumption is due to data transmission. For that we apply Data aggregation approach on the sensed data by the deployed sensor nodes. This approach helps to reduce the number of transmissions and improves the life time of wireless sensor network with less energy usage of sensor nodes and also to protect Data Aggregation process from various kinds of attacks becomes extremely critical. So we give some general framework for Secure Data Aggregation.

Keywords: Wireless Sensor Network, Sink Node, Security, Attacks, Cluster, Data Aggregation.

I. INTRODUCTION

Wireless Sensor Networks are being employed in various real time fields like military, disaster management, Industry, Environmental Monitoring and Agriculture Farming etc. Due to diversity of so many real time scenarios, security for WSNs becomes a complex issue. For each implementation, there are different type of attacks possible and demands a different security level. Major challenge for employing an efficient security scheme comes from the resource constrained nature of WSNs like size of sensors, Memory, Processing Power, Battery Power etc. and easy accessibility of wireless channels by good citizens and attackers.

Wireless sensor networks are usually deployed at unattended or hostile environments. Therefore, they are very vulnerable to various security attacks, such as selective forwarding, wormholes, and sybil attacks. In addition, wireless sensor networks may also suffer from injecting false data attack. For an injecting false data attack, an adversary first compromises several sensor nodes, accesses all keying materials stored in the compromised nodes, and then controls these compromised nodes to inject bogus information and send the false data to the sink to cause upper level error decision, as well as energy wasted in en-route nodes. The Sensor Network can be described as a collection of sensor nodes which co-ordinate to perform some specific action. Unlike traditional networks, sensor networks depend on dense deployment and co-ordination to carry out their tasks. Sensor Networks consisted of small number of sensor nodes that were wired to a central processing station. However, nowadays, the focus is more on Wireless Sensor Networks.

Sensor networks are collection 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.

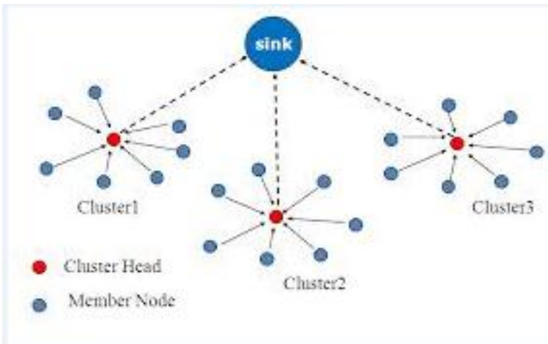

Figure.1 Data Aggregation

Figure.2 shows Wireless Sensor Network Architecture. Wireless sensor networks are consisting of numerous light weight and tiny sensor nodes with limited power, storage, communication and computation capabilities. Wireless sensor networks are being employed in civilian applications like habitat monitoring to mission critical Applications.

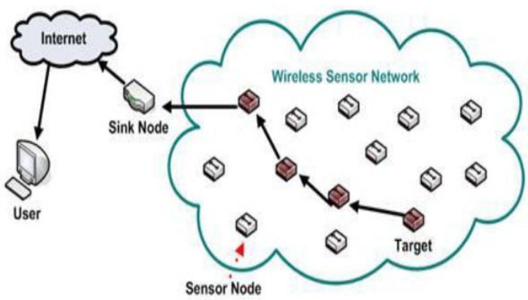

Figure.2 Wireless Sensor Network Architecture

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

II. LITERATURE REVIEW

The literature review covers the background, latest development of and related techniques for secure data aggregation in Wireless Sensor Network (WSN). Data Aggregation is the process of combining the partial result at intermediate node during message routing in WSN. Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.
We have to analysis the Parallel and distributed systems Survey**:**

Parallel and distributed computing
-"A distributed system is a collection of independent computers that appear to the users of the system as a single computer."
-"A distributed system consists of a collection of autonomous computers linked to a computer network and equipped with distributed system software."
-"A distributed system is a collection of processors that do not share memory or a clock."
-"Distributed systems are a term used to define a wide range of computer systems from a weakly-coupled system such as wide area networks, to very strongly coupled systems such as multiprocessor systems."
Distributed systems are groups of networked computers, which have the same goal for their work. The terms "concurrent computing", "parallel computing", and "distributed computing" have a lot of overlap, and no clear distinction exists between them. The same system may be characterized both as "parallel" and "distributed"; the processors in a typical distributed system run concurrently in parallel. Parallel computing may be seen as a particular tightly-coupled form of distributed computing, and distributed computing may be seen as a loosely-coupled form of parallel computing. Nevertheless, it is possible to roughly classify concurrent systems as "parallel" or "distributed" using the following criteria:
-In parallel computing, all processors have access to a shared memory. Shared memory can be used to exchange information between processors.
-In distributed computing, each processor has its own private memory (distributed memory). Information is exchanged by passing messages between the processors.

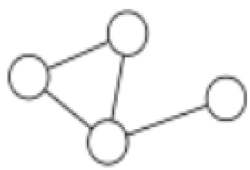

Figure3 (a) Distributed System

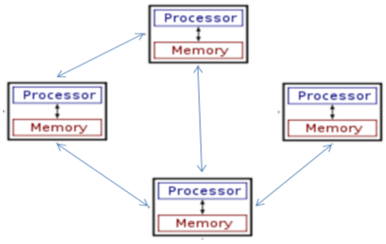

Figure.3 (b) Distributed System

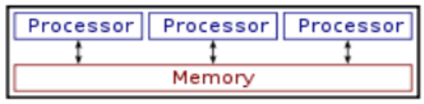

Figure.4 Parallel System

The figure on the right illustrates the difference between distributed and parallel systems. Figure 3(a) is a schematic view of a typical distributed system; as usual, the system is represented as a network topology in which each node is a computer and each line connecting the nodes is a communication link. Figure 3(b) shows the same distributed system in more detail: each computer has its own local memory, and information can be exchanged only by passing messages from one node to another by using the available communication links. Figure 4 shows a parallel system in which each processor has a direct access to a shared memory.

III. PROPOSED METHODOLOG AND DISCUSSION

In this paper, we propose a novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data. Based on the random graph characteristics of sensor node deployment and the cooperative bit-compressed authentication technique, the proposed BECAN scheme can save energy by early detecting and filtering the majority of injected false data with minor extra overheads at the en-route nodes. In addition, only a very small fraction of injected false data needs to be checked by the sink, which thus largely reduces the burden of the sink. Both theoretical and simulation results are given to demonstrate the effectiveness of the proposed scheme in terms of high filtering probability and energy saving.
A statistical en-routing filtering mechanism called SEF. SEF requires that each sensing report be validated by multiple keyed message authenticated (MACs), each generated by a node that detects the same event. In SEF, to verify the MACs, each node gets a random subset of the keys of size k from the global key pool of size N and uses them to producing the MACs. To save the bandwidth, SEF adopts the bloom filter to reduce the MAC size. By simulation, SEF can prevent the injecting false data attack with 80-90 percent probability within 10 hops. SEF does not consider the possibility of en-routing nodes' compromise, which is also crucial to the false data filtering. Present an interleaved hop-by-hop authentication (IHA) scheme for filtering of injected false data. In IHA, each node is associated with two other nodes along the

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

path, one is the lower association node, and the other is the upper association node. An en-routing node will forward receive report if it is successfully verified by its lower association node. To reduce the size of the report, the scheme compresses t + 1 individual MACs by XORing them to one. By analyses, only if less than t nodes are compromised, the sink can detect the injected false data. However, the security of the scheme is mainly contingent upon the creation of associations in the association discovery phase. Once the creation fails, the security cannot be guaranteed.

Sensor Node Initialization
In this technique, the key server generates unique public and private keys for each sensor node and sink. These keys will be shared to the sensor nodes when they start.

CNR Based MAC Generation
This technique is used by the sensor nodes for generating authentication message. This technique uses Elliptic curve cryptography and DES algorithm.

CNR Based MAC Verification
In this phase, the sink verifies the authentication message sent by sensor node using ECC algorithm.

Sink Verification
In this module, the sink verifies each message sent by sensor nodes weather it is valid or invalid.

Elliptic Curve Cryptography (ECC)
It is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems, such as the RSA algorithm, are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly-known base point is infeasible. The size of the elliptic curve determines the difficulty of the problem. It is believed that the same level of security afforded by an RSA-based system with a large modulus can be achieved with a much smaller elliptic curve group. Using a small group reduces storage and transmission requirements.

Let p be a large prime and E(IFp)represent an elliptic curve defined over IFp. Let G €E(IFp)be a base point of prime order q. Then, each sensor nodeNi € N can preload a TinyECC based public-private key pair (Yi, xi), where the private key xi is randomly chosen from Z*q and the public key Yi =xi, G. No interactive key pair establishment. For any two sensor nodes vi, vj€ G = (V,έ) no matter what eij€{0,1} is, sensor nodes vi with the key pair (Yi, xi) and vj with the key pair (Yj,xj) can establish a secure Elliptic Curve Diffie-Hellman (ECDH) key pair without direct contacting, where kij=xiYj=xixjG=xjxiG=xjYi=kji. vi and vj can secretly share a key. At the same time, the established keys are independent. In other words, if a sensor node vi is compromised, then the key kij shared between vi and vj will be disclosed. However, the key kjj` shared between vj and another sensor node vj` is not affected.

Design Rationale
To filter the false data injected by compromised sensor nodes, the BECAN adopts cooperative neighbor router (CNR) based filtering mechanism. As shown in Fig. 5 CNR-based mechanism, when a source node N0 is ready to send a report m to the sink via an established routing path RN0: [R1 -> R2 ->. . Rl-> Sink], it first resorts to its k neighboring nodes NN0: {N1, N2, . ..,Nk} to cooperatively authenticate the report m, and then sends the report m and the authentication information MAC from N0 U NN0 to the sink via routing RN0.

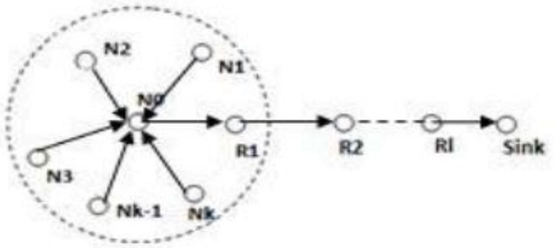

Figure.5 Cooperative CNR-Based authentication mechanism

IV. EXPERIMENTAL EVALUATION

Secure data aggregation by early detecting false data:
The sink is a powerful data collection device. Nevertheless, if all authentication tasks are fulfilled at the sink, it is undoubted that the sink becomes a bottleneck. At the same time, if too many injected false data flood into the sink, the sink will surly suffer from the Denial of Service (DoS) attack. Therefore, it is critical to share the authentication tasks with the en-route sensor nodes such that the injected false data can be detected and discarded early. The earlier the injected false data are detected, the more energy can be saved in the whole network.

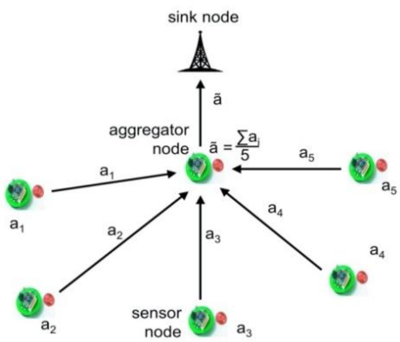

Figure.6. Data Aggregation

Example : At the same time, if all false data are flooding into the sink simultaneously, then not only huge energy will be wasted in the en-route nodes, but also heavy verification burdens will undoubtedly fall on the sink. As a result, the whole network could be paralyzed quickly. Therefore, filtering false data should also be executed as early as possible to mitigate the energy waste. To tackle this challenge issue, some some false data filtering mechanisms have been developed. Since most of these filtering mechanisms use the symmetric key technique,

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

once a node is compromised, it is hard to identify it. In other words, the compromised node can abuse its keys to generate false reports, and the reliability of the filtering mechanisms will be degraded.

V. IMPLEMENTATION

BECAN Scheme

A novel bandwidth-efficient cooperative authentication (BECAN) scheme for filtering injected false data in wireless sensor networks. Compared with the previously reported mechanisms, the BECAN scheme achieves not only high filtering probability but also high reliability.

-First, we study the random graph characteristics of wireless sensor node deployment, and estimate the probability of k-neighbors, which provides the necessary condition for BECAN authentication.

-Second, we propose the BECAN scheme to filter the injected false data with cooperative bit-compressed authentication technique. With the proposed mechanism, injected false data can be early detected and filtered by the en-route sensor nodes. In addition, the accompanied authentication information is bandwidth-efficient; and

-Third, we develop a custom simulator to demonstrate the effectiveness of the proposed BECAN scheme in terms of en-routing probability and false negative rate true reports.

Therefore, it is crucial to filter the false data as accurately

A wireless sensor network is usually composed of a large number of sensor nodes which are interconnected through wireless links to perform distributed sensing tasks. Each sensor node is low-cost but equipped with necessary sensing, data processing, and communicating components. Therefore, when a sensor node generates a report after being triggered by a special event, e.g., a surrounding temperature change, it will send the report to a data collection unit (also known as sink) through an established routing path. Wireless sensor networks are usually deployed at unattended or hostile environments. Therefore, they are very vulnerable to various security attacks, such as selective forwarding, wormholes, and sybil attacks. In addition, wireless sensor networks may also suffer from injecting false data attack. For an injecting false data attack, an adversary first compromises several sensor nodes, accesses all keying materials stored in the compromised nodes, and then controls these compromised nodes to inject bogus information and send the false data to the sink to cause upper level error decision, as well as energy wasted in en-route nodes. For instance, an adversary could fabricate a wildfire event or report wrong wildfire location information to the sink, then expensive resources will be wasted by sending rescue workers to a non-existing or wrong wildfire location.

As possible in wireless sensor networks.

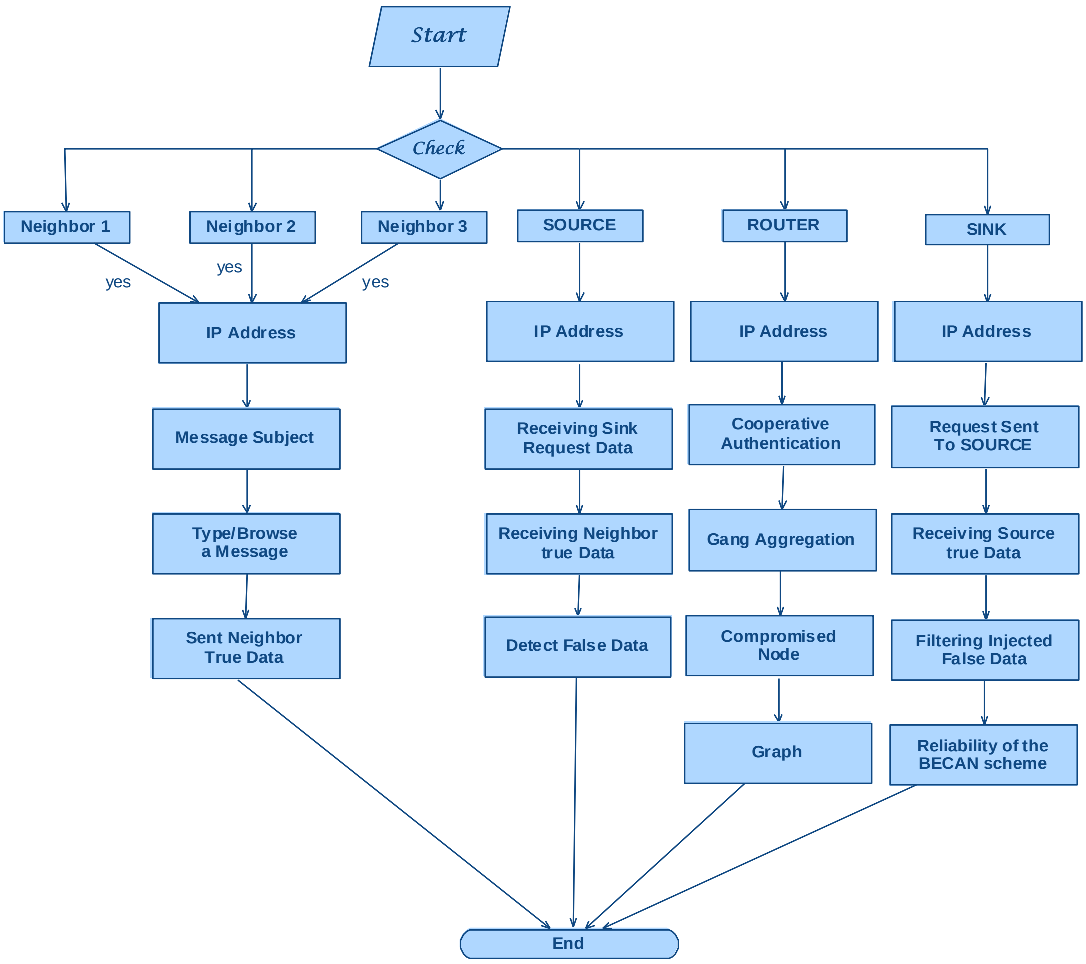

Figure.7 Data Flow Diagram

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

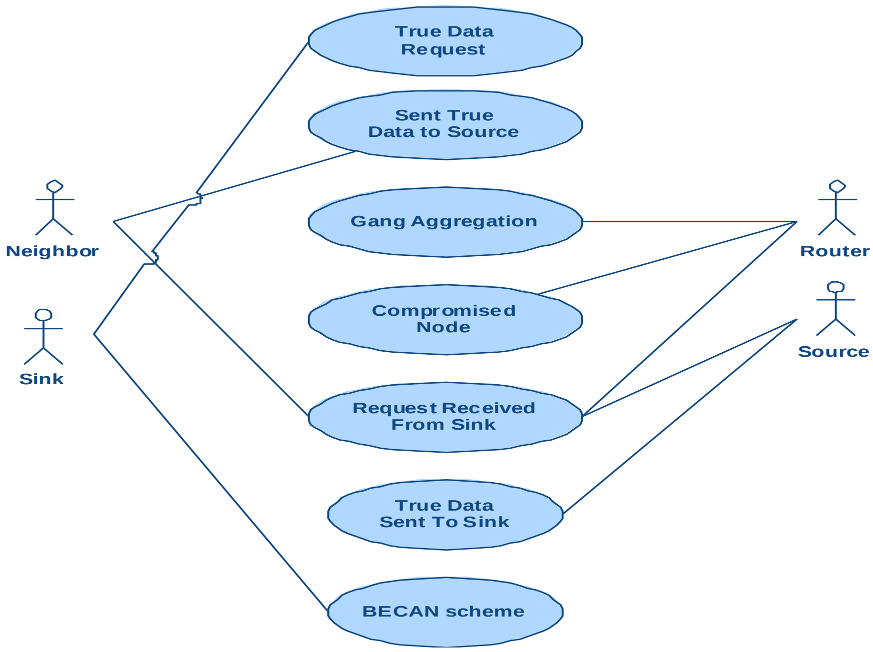

Figure.8 Use Case Diagram

Work Flow

Step 1: Sink device is sending request to sources. In this 3 clients will send three requests to source.
Step 2: neighbor 1/2/3 will send message to sources
Step 3: while transforming the data, if all data where at purest form –no problem will arise.
Step 4: while transferring data, router will get activated and transfer the data (source to sink)
Step 5: secure aggregation of data will be at sink, sink device provide high security.

VI. CONCLUSION

In this paper, we have proposed secure data aggregation by using sink device and elaborated a novel bandwidth scheme efficient cooperative authentication (BECAN) scheme for filtering the injected false data. By theoretical analysis and simulation evaluation, the BECAN scheme has been demonstrated to achieve not only high en-routing filtering probability but also high reliability with multi reports. Due to the simplicity and effectiveness, the BECAN scheme could be applied to other fast and distributed authentication scenarios, e.g., the efficient authentication in wireless mesh network. In our future work we will investigate how to prevent the gang injecting false data attack from mobile compromised sensor nodes.

ACKNOWLEDGEMENT

My thanks to the Guide, **Prof. K. G. Badge** and Principal **Dr. A. B. Marathe**, who provided me constructive and positive feedback during the preparation of this paper.

REFERENCES

[1] Sankardas Roy, Mauro Conti, Sanjeev Setia, and Sushil Jajodia, "Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact", IEEE Transactions On information forensics and security, vol. 9, no. 4, april 2014.
[2] V. Chitra, L.Hameetha Begum, M. Ramya, R. Udhaya," Filtering False Data Injection Using Becan Scheme in Wireless Sensor Networks", IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014.
[3] Amuthan Mathy.P, Gowri Sankar.U, "Filtering Injected False Data in Wireless Sensor Networks by Using L, F, S Nodes and Key Distribution", International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1, March 2014.
[4] Laxmi Shabadi, Snehal .T, Sanjana .H, Kalavati .G, Anita .K, "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data using timer in Wireless Sensor Networks", International Journal of Emerging Engineering Research and Technology Volume 2, Issue 3, June 2014.
[5] Xinyu Yang, Jie Lin, Paul Moulema,Wei Yu, Xinwen Fu and Wei Zhao, "A Novel En-route Filtering Scheme against False Data Injection Attacks in Cyber-Physical Networked Systems", 2012 32nd IEEE International Conference on Distributed Computing Systems
[6] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui Liang, and Xuemin (Sherman) Shen, Fellow, "BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 23, NO. 1, JANUARY 2012

BIOGRAPHIES

Miss. Priyanka G Padmane, received the B.E. degree in Information Technology from H.V.P.M's College Of Engineering And Technology, Amravati in 2013. She is currently perusing Master's Degree in Computer Science and Information Technology from H.V.P.M's College of Engineering And Technology, Amravati.

Prof. K.G. Bagde, received the B.E. and M.E degree in Computer Science from Prof.Ram Meghe College of Engineering And Technology, Amravati. Her field of specialization is networking. She is currently working as Associate Professor at H.V.P.M's college of Engineering and Technology, Amravati.