A Privacy-Preserving Location Monitoring System for WSNs with Blocking Misbehaving Users in Anonymity Networks

Kirankumar B. Balavalad, Ajayakumar C. K. Atageri, Prithviraj. S. Patil, and Basavaraj M. Angadi

***Abstract*—Wireless sensor networks monitoring personal locations are identified through internet server. If server is untrusted, it may cause threats pertaining to privacy of individuals being monitored. In this work, we propose a privacy preserving location monitoring system for wireless sensor networks. Here, we design two in-network anonymization algorithms which aim to enable the system to provide high quality location monitoring services, while preserving personal location privacy and algorithms rely on the well-established n-anonymity privacy concept. For the location monitoring system using identity sensors, the sensor nodes report the exact location information of the monitored persons to the server; thus using identity sensors immediately poses 3 major privacy breaches. To tackle such a privacy breach, the concept of aggregate location information, that is, a collection of location data relating to a group or category of persons from which individual identities have been removed has been suggested as an effective approach to preserve location privacy.**

***Index Terms*—Wireless sensor network location monitoring, privacy preservation anonymity network resource aware, quality aware.**

I. Introduction

Wireless sensor networks rely on wireless communication, which is by nature a broadcast medium that is more vulnerable to security attacks than its wired counterpart due to lack of a physical boundary. In the wireless sensor domain, location privacy is an important security issue. Lack of location privacy can expose significant information about the traffic carried on the network and the physical world entities. Various protocols are proposed for routing and data gathering but none of them are designed with security as a goal. The resource limitation of sensor networks poses great challenges for security. The security breaches occur primarily in the form of Interruption, Interception, Modification and fabrication. Few of the security attacks are Denial of service, Attack of information in transit, Sybil attack, Blackhole/ Sinkhole Attack, 'Hello flood' Attack, Wormhole Attack.

Privacy has been a major security issue in WSN's, which can be classified into Data-oriented and Context-oriented [1], [2]. Data-oriented protections are categorized into data aggregation and data query techniques. Context-oriented privacy protections can be split into location privacy and temporal privacy techniques, the location privacy is split into data source and base station techniques. [1] This paper provides an overview of ongoing research activities, various design issues involved and possible solutions incorporating these issues. This paper [2] explains WSN is an emerging technology that shows great promise for various futuristic applications both for mass public and military and studies the security aspects of these networks. The paper [3] discusses about classification of WSN and challenges of the Next Generation WSN. The paper [4] says increasing demand for security and automated monitoring of things and places makes WSNs a promising technology. [5] Says monitoring personal locations with a potentially untrusted server poses privacy threats to the monitored individuals. The [6] author takes an example such as a hospital or bank, needs to share person-specific records in such a way that the identities of the individuals who are the subjects of the data cannot be determined. [7] Proposes an anonymous communication technique to protect the location privacy of the users of location-based services. [8] Paper tackles a major privacy threat in current location-based services where users have to report their exact locations to the database server in order to obtain their desired services. In this paper, we propose a privacy preservation of such mobile users with the help of anonymization and by reporting aggregate location. An anonymization means a person is indistinguishable amongst k persons in a network. The most effective way to compromise location privacy used by adversary is packet-tracing. In such an attack, an adversary can locate the immediate nodes by eavesdropping the transmitted packet, and further reduce the flow direction of packets. Along with privacy preservation of mobile users we are monitoring location of any mobile user through our system.

Manuscript received December 26, 2013; revised June 14, 2014. This work was supported and sponsored by World Bank project, TEQIP phase-II.

The authors are with Basaveshwar Engineering College Bagalkot, Karnataka, India (e-mail: kiranb4004@gmail.com, ajaykatageri@yahoo.co.in, balajibiradar64@gmail.com, basavaraj.914@gmail.com).

II. Existing System

The existing system [5]-[8] is based on the concepts like, **False Locations**, **Spatial Cloaking** and **Space Transformation**. Anonymous communications will provide anonymous routing between the sender and the receiver. Source location privacy hides the sender's location and identity. Aggregate data privacy that preserves the privacy of the sensor node's aggregate readings during transmission. Data storage privacy hides the data storage location. Query privacy that avoids disclosing the personal interests. Drawbacks of the Existing System are, False location technique, Space transformation technique, Spatial cloaking technique.

DOI: 10.7763/JACN.2014.V2.121

III. Proposed Work

A. Problem Definition

Individuals whose personal location is being monitored by a third party, are vulnerable to privacy threats. To address this problem, servers can "blacklist" misbehaving users, thereby blocking users without compromising their anonymity. For the location monitoring system using identity sensors, the sensor nodes report the exact location information of the monitored persons to the server, thus using identity sensors immediately poses a major privacy breach.

B. System Model

Fig. 1 depicts the architecture [6]-[8] of our system, where there are three major entities, sensor nodes, server, and system users.

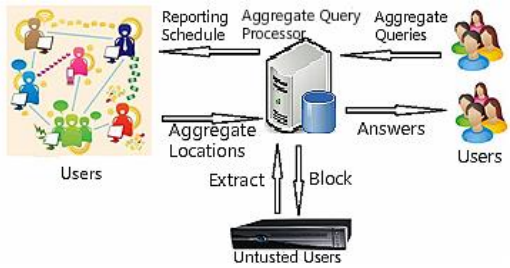

Fig. 1. System architecture.

1) Sensor nodes

Each sensor node determine the number of objects in its sensing area, then blurs its sensing area into a cloaked area 'm', which includes at least 'n' objects, and reporting 'm' with the number of objects located in 'm' as aggregate location information to the server.

2) Resource-based blocking

To limit the number of identities a user (Ex: Alice), we have used IP address as resource in our implementation.

3) Server

Server will collect the aggregate locations reported from the sensor nodes, using a spatial histogram to estimate the distribution of the monitored objects, and answering range queries based on the estimated object distribution.

4) System users

Here only authenticated administrators and users can issue range queries to our system through either the server or the sensor nodes. The server uses the spatial histogram to answer their queries.

5) Privacy model

In our system, the sensor nodes constitute a cloaked area and works as defined in our algorithm and communicate with each other through a secure network channel to avoid internal network attacks. Our system also provides anonymous communication between the sensor nodes and the server by employing existing anonymous communication techniques.

6) The pseudonym manager

User must first contact the Pseudonym Manager (PM) and demonstrate control over a resource; for IP-address blocking, the user must connect to the PM directly.

7) The nymble manager

As the PM provided pseudonym to the user and the user connects to the Nymble Manager (NM) through the anonymizing network, and requests nymbles for access to a particular server (such as Google). These nymbles are thus specific to a particular user-server pair.

8) Time

Nymble tickets are bound to specific time periods. While a user's access within a time period is tied to a single nymble ticket, the use of different nymble tickets across time periods grants the user anonymity between time periods. Smaller time periods provide users with higher rates of anonymous authentication, while longer time periods allow servers to rate-limit the number of misbehaviors from a particular user before he or she is blocked and are blacklisted.

9) Blacklisting a user

If a user misbehaves, the server may link any future connection from this user within the current likability window. A user connects and misbehaves at a server during time period t within likability window w. The server later detects this misbehavior and complains to the NM in time period tc of the same likability window w. As part of the complaint, the server presents the nimble ticket of the misbehaving user and obtains the corresponding seed from the NM. The server is then able to link future connections by the user in time periods of the same likability window w to the complaint. Therefore, once the server has complained about a user, that user is blacklisted for the rest of the day.

IV. Proposed Algorithms

In this section, I present an in-network resource and quality-aware location anonymization algorithms that is periodically executed by the sensor nodes to report their k-anonymous aggregate locations to the server for every reporting period.

A. The Resource-Aware Algorithm

The resource-aware algorithm aims to minimize communication and computational cost, while the quality-aware algorithm aims to minimize the size of cloaked areas in order to generate more accurate aggregate locations. To provide location monitoring services based on the aggregate location information, we propose a *spatial histogram* approach that analyzes the aggregate locations reported from the sensor nodes to estimate the distribution of the monitored objects. The estimated distribution is used to provide location monitoring services through answering range queries. We evaluate our system through simulated experiments.

The main idea of the Resource aware algorithm is to find adequate number of persons in that network and accordingly finding a cloaked area as MBR (minimum bounded area).

1) Broadcast step

In this step, every sensor node in a network broadcasts a message which contains id, area and number of nodes to its nearest neighbor. In this way every sensor node forms its own table and also checks for adequate number of objects in its sensing area and accordingly it sends notification message to

the nearer sensor nodes and follows the next step.

2) Cloaked area step

The basic idea of this step is that each sensor node blurs its sensing area into a cloaked area that includes at least k objects, in order to satisfy the k-anonymity privacy requirement. To minimize computational cost, it uses a greedy approach to find a cloaked area based on the information stored in table. Each sensor node initializes a set S and then determines a score for each peer in its table. The score is defined as a ratio of the object count of the peer to the distance between the peer and node. The score is calculated to select a set of peers from table to S to form a cloaked area that includes at least k objects and has an area as small as possible. Then we repeatedly select the peer with the highest score from the table to S until S contains at least k objects. Finally, node determines the cloaked area that is a minimum bounding rectangle that covers the sensing area of the sensor nodes in S, and the total number of objects in S.

3) Validation step

Validation step is used to avoid reporting aggregate locations with a containment relationship to the server. We do not allow the sensor nodes to report their aggregate locations with the containment relationship to the server, because combining these aggregate locations may pose privacy leakage.

Algorithm 1: Resource-Aware Location Anonymization
1: function *R*.AWARE (Integer *k*, Sensor *m*, List *R*)
2: Peer List (initially 0)

// **Step 1: The broadcast step**
3: First send a message with m's identity, sensing area, and object count (m:ID, m:Area, m:Count to m's neighbour peers)
4: in return if Receive a message from a peer p, i.e., (p:ID, p:Area, p:count) then
5: The message will be added to Peer List
6: if adequate numbers of objects are found in m then
7: Notification message is sent to m's neighbours
8: end if
9: if some m's neighbour has not found an adequate number of objects then
10: Forward the message to m's neighbours cloaked area
11: end if
12: end if

// **Step 2: The cloaked area step**
13: $S \longleftarrow \{m\}$ (area to cloaked area)
14: a score for each peer in Peer List is computed
15: Repeatedly select the peer with the highest score from Peer List to *S* until the total number of objects in *S* is at least *k*
16: a MBR of the senor nodes in S then
17: N will be total number of objects in S

// **Step 3: The validation step**
18:*R*← Aggregate reporting
if $R \in R$ then No containment relationship with Area
19: Now send a message (*S*; *N*) to the peers within Area and the server
20: else if the m's sensing area is contained by some report then
21: Select a $Rs \in R$ (*Rs*←random select) such that R': S contains m's sensing area
22: Now send this *Rs* to the peers within *Rs* Area and the server
23: else
24: Send S with a cloaked N to the peers within Area and the server
25: end if

B. Quality Aware Algorithm

The quality-aware algorithm starts from a cloaked area A, which is computed by resource aware algorithm. Then A will be iteratively updated based on extra communication among the sensor nodes until its area reaches the minimal possible size. For both algorithms, the sensor node reports its cloaked area with the number of monitored persons in the area as an aggregate location to the server.

1) Search space step

Sensor network has a large number of sensor nodes hence it is very costly for a sensor node to gather the information of all the sensor nodes to compute its minimal cloaked area. To reduce the cost, node determines a search space based on the input cloaked area computed by the resource-aware algorithm.

2) The minimal cloaked area step

This step takes a set of peers residing in the search space, S, as an input and computes the minimal cloaked area for the sensor node m. The basic idea of the first optimization technique is that we do not need to examine all the combinations of the peers in S, instead we only need to consider the combinations of at most four peers. Because at most two sensor nodes defines width of MBR and at most two sensor nodes defines height of MBR. It reduces cost by reducing the number of MBR computations among the peers in S.

3) The validation step

This step is to avoid reporting aggregate locations with a containment relationship to the server. We do not allow the sensor nodes to report their aggregate locations with the containment relationship to the server, because combining these aggregate locations may pose privacy leakage.

Algorithm 2: Quality-Aware Location Anonymization
1: function Q.AWARE (Int *k*, Sensor *m*, Set init_solution, List R)
2: current_min_cloaked _area init_solution

// **Step 1: The search space step**
3: First search space area S based on the initial solution
4: Assemble the peers information located in S

// **Step 2: The minimal cloaked area step**
5: each peer located in *S* to *C*[*i*] is added as an item
6: then m to each item set in *C*[*i*] is added as the first item
7: for $i = 1$(initial); $i <= 4$; i ++
8: every item set $I = \{a1, \ldots\ldots, ai+1\}$ in *C*[*i*]
9: if *S* (*Z*) < *S* (current min cloaked area) then
10: if *N* (*Z*) >=*k*
11: then current min cloaked area= {*Z*}
12: Remove *Z* from *C*[*i*]
13: end if;

14: else
15: end for;
16: if $i < 4$ then
17: for item set pair $Z=\{z1, .,z\ i+1\}$, $Y=\{y1, \ldots, yi+1\}$ in $C[i]$
18: do if $z1 = y1, \ldots\ldots, zi = yi$ and $zi+1 != yi+1$ then
19: Add an item set $\{z1, \ldots..,zi+1; yi+1\}$ to $C[i + 1]$
20: end if;
21: end for;
22: $S(Z)$ a MBR of current min cloaked area
23:$N(Z)$ the total number of object in current_min_cloaked_area

// Step 3: The validation step
25:$R\leftarrow$ Aggregate reporting
if R ∈ R then No containment relationship with Area
26: Now send a message (S; N) to the peers within Area and the server
27: else if the m's sensing area is contained by some report then
28: Select a Rs ∈ R (Rs←random select) such that
R': S contains m's sensing area
29: Now send this Rs to the peers within Rs Area and the server
30: else
31: Send S with a cloaked N to the peers within Area and the server
32: end

V. Simulation

A. Simulation Model

1) Sensor nodes

Each sensor node is responsible for determining the number of objects in its sensing area, blurring its sensing area into a cloaked area A, which includes at least k objects, and reporting A with the number of objects located in A as aggregate location information to the server. Each sensor node is also aware of its location and sensing area.

2) Resource-based blocking

To limit the number of identities a user can obtain, the Nymble system binds to resources that are sufficiently difficult to in great numbers. For ex. We have used IP address as resource in our implementation.

3) Server

The server is responsible for collecting the aggregate locations reported from the sensor nodes, using a spatial histogram to estimate the distribution of the monitored objects, and answering range queries based on the estimated object distribution. Furthermore, the administrator can change the anonymized level k of the system at anytime by disseminating a message with a new value of k to all the sensor nodes.

4) System users

Authenticated administrators and users can issue range queries to our system through either the server or the sensor nodes, as depicted in Fig. 2. The server uses the spatial histogram to answer their queries.

5) Privacy model

In our system, the sensor nodes constitute a trusted zone, where they behave as defined in our algorithm and communicate with each other through a secure network channel to avoid internal network attacks. Our system also provides anonymous communication between the sensor nodes and the server by employing existing anonymous communication techniques. Thus given an aggregate location R, the server only knows that the sender of R is one of the sensor nodes within R. Furthermore, only authenticated administrators can change the k-anonymity level and the spatial histogram size. In emergency cases, the administrators can set the k-anonymity level to a small value to get more accurate aggregate locations from the sensor nodes, or even set it to zero to disable our algorithm to get the original readings from the sensor nodes, in order to get the best services from the system.

VI. Results

Fig. 2-Fig. 9 show the experimental results with respect to the privacy protection and the quality of location monitoring services of our system.

Fig. 2. Location monitoring output.

Fig. 4. User location monitoring.

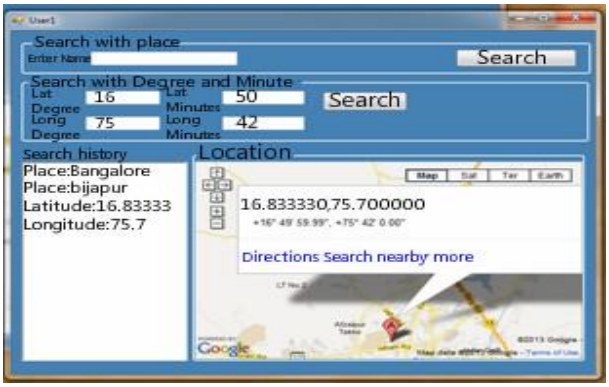

Fig. 5. Location monitoring (Google map).

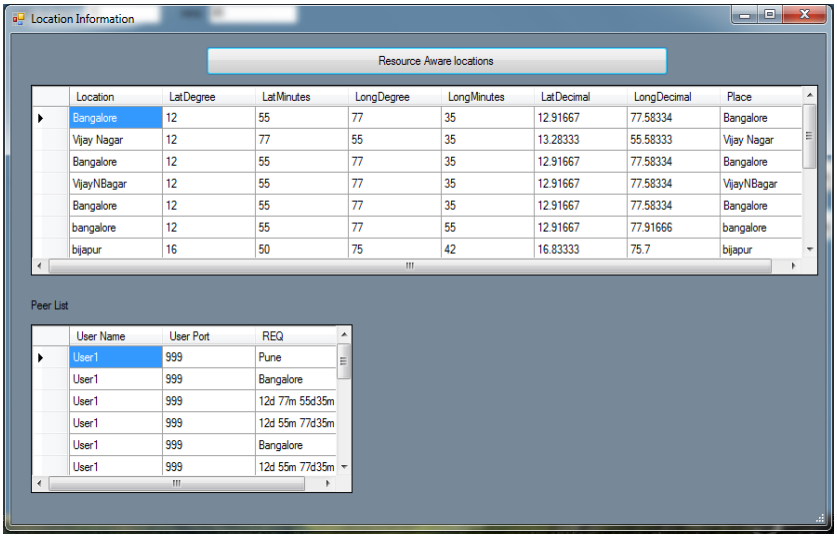

Fig. 3. Resource aware locations.

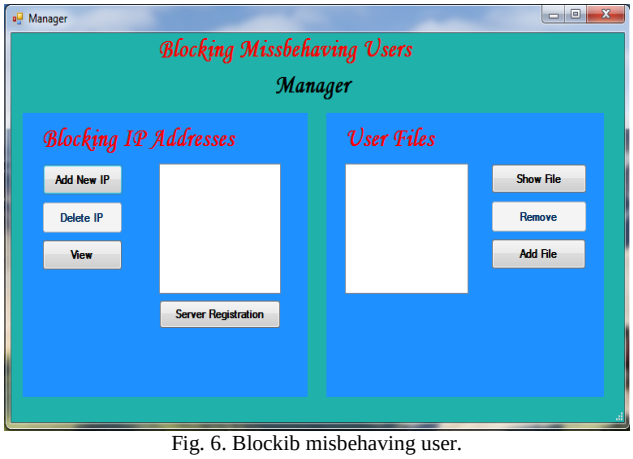

Fig. 6. Blockib misbehaving user.

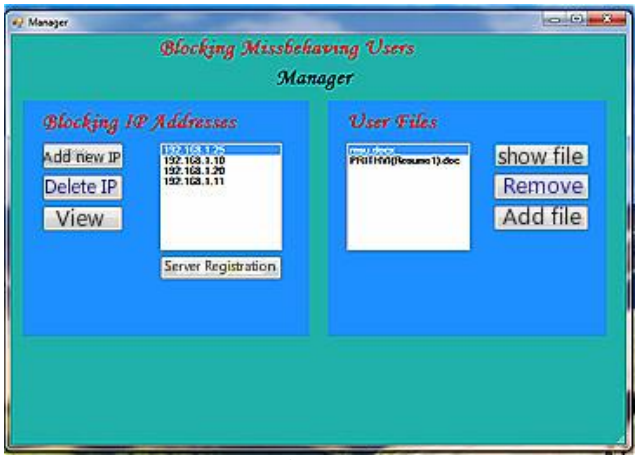

Fig. 7. List of blocked IP address.

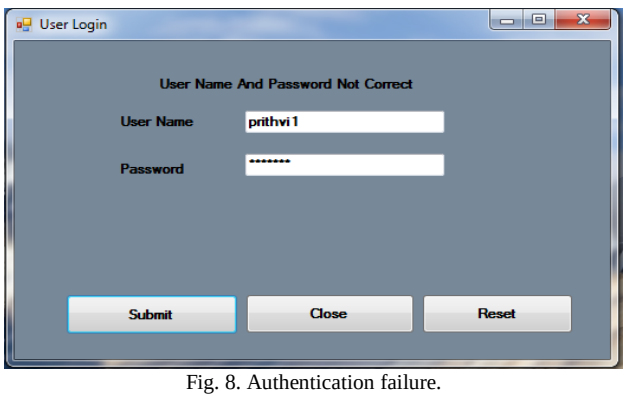

Fig. 8. Authentication failure.

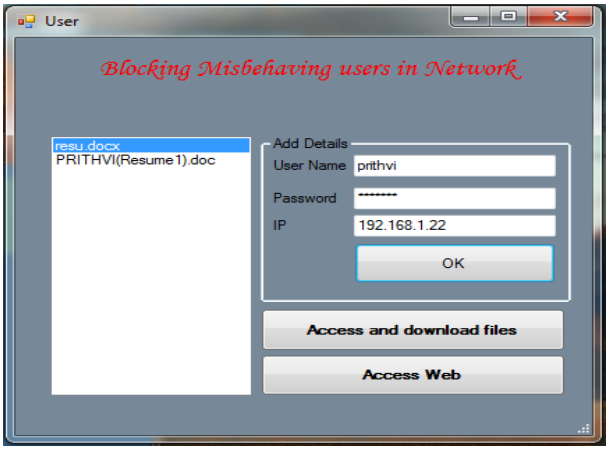

Fig. 9. Blocking misbehaving in network.

VII. Conclusion

In this paper, we propose a privacy-preserving location monitoring system and data protection privacy for wireless sensor networks with blocking misbehaving users. We adopt two in-network location anonymization algorithms, namely resource and quality-aware algorithms that preserve personal location privacy and data protection, while enabling the system to provide location monitoring services. The resource aware algorithm mainly aims to minimize the communication and computational cost, whereas quality aware aims to minimize the cloaked area. This paper also provides data privacy from unauthorized users. The data protection provides security to documents, files, etc. The results show that system provides high quality location monitoring and data protection privacy services. In this system servers can blacklist the misbehaving users (unauthorized) from network.

References

[1] S. Gowrishankar, T. G. Basavaraju, D. H. Manjaiah, and S. K. Sarkar, "Issues in wireless sensor networks," *Proceedings of the World Congress on Engineering*, vol. 1, July 2-4, 2008.

[2] D. N. Sushma and V. Nandal, "Security threats in wireless sensor networks," *International Journal of Computer Science & Management Studies*, vol. 11, issue 1, May 2011.

[3] N. Srivastava, "Challenges of next-generation wireless sensor networks and its impact on Society," *Journal of Telecommunications*, vol. 1, issue 1, Feb 2010.

[4] S. A. Rua and A. Cordeiro, "Sensing the World: Challenges on WSNs," Vâlter RochaInstituto Agilus de Inovação em Tecnologia de Informação, Matosinhos Portugal.
[5] C. Y. Chow, M. F. Mokbel, and T. He, *A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks*.
[6] L. Sweeney, "Achieving *K*-Anonymity Privacy Protection Using Generalization and Suppression," School of Computer Science, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA.
[7] *An Anonymous Communication Technique Using Dummies for Location-Based Services*, NTT Corporation.
[8] C. Y. Chow, M. F. Mokbel, X. Liu, and T. J. Watson, *A Peer-To-Peer Spatial Cloaking Algorithm For Anonymous Location-Based Services*, Research Center Hawthorne, NY.

Kirankumar B. Balavalad was born on November 8, 1985, grown in Bagalkot, Karnataka, India. He completed his BE degree in electronics & communication engineering in 2008 from Basaveshwar Engineering College, Bagalkot, Karnataka, India, under the Vishveshwarayya Technological University, Belgaum, India. Then received his master of technology in digital communication, from Basaveshwar Engineering College, Bagalkot, in 2010. He is currently pursuing his PhD degree in the area of MEMS, from Vishveshwarayya Technological University, Belgaum, India.

He is currently working as an assistant professor in Department of Electronics & Communication Engineering, Basaveshwar Engineering College, Bagalkot, Karnataka, India.

Prof. Kirankumar is a life member of ISSS, UACEE, & member of IEEE.

Ajayakumar C. Katageri was born on July 21st, 1985, and grown in Bagalkot, Karnataka, India. He completed his BE degree in E&C field in 2008 from Basaveshwar Engineering College Bagalkot, Karnataka, India. Then received his master of technology in digital communication from Basaveshwar Engineering College, Bagalkot, in 2010. He is perusing his PhD degree in the area of MEMS.

He is currently working as an assistant professor in Department of E&CE, Basaveshwar Engineering College, Bagalkot, Karnataka, India.

Prof. Katageri is a life member of ISSS, UACEE, & member of IEEE.

Basavaraj M. Angadi was born on July 1st, 1987, and grown in Bagalkot city, Karnataka state, India. He completed his BE degree of E&C field in 2009 from Basavakalyan Engineering College Basavakalyan, Karnataka state, India. And he is pursuing master of technology in digital electronics and communication field from Basaveshwar engineering college, Bagalkot He is currently working as an assistant professor in Department of E&CE, Basaveshwar Engineering College, Bagalkot, Karnataka, India.