# FAULTY NODE DETECTION IN DELAY TOLERANT NETWORKS

**Mr.P.V.R.K.MURTHY[1], A.LAKSHMI SUPRIYA[2]**

**[1]Associate Professor,Dept of MCA,Audisankara College of Engineering & Technology (AUTONOMOUS), Gudur, AP,India.**

**[2]PG Scholar,Dept of MCA,Audisankara College of Engineering & Technology (AUTONOMOUS), Gudur, AP,India.**

**ABSTRACT_** a fully distributed and easily implementable approach to allow each DTN node to rapidly identify whether its sensors are producing faulty data.

The dynamical behavior of the proposed algorithm is approximated by some continuous-time state equations, whose equilibrium is characterized.

The presence of misbehaving nodes, trying to perturb the faulty node detection process, is also taken into account. Detection and false alarm rates are estimated by comparing both theoretical and simulation results.

## 1.INTRODUCTION

DELAY Tolerant Networks (DTN) are challenging networks with frequent disconnections and a dynamic topology [1]. Instances of DTNs incorporate Vehicular DTNs (VDTNs) [2] where two hubs can speak with one another just when they are firmly found. This association is discontinuous as the hubs are moving vehicles. Because of this meager and irregular availability, deduction and learning over DTNs is significantly more convoluted than in customary organizations, see, e.g., [3], [4], [5], [6], [7], [8]. This paper thinks about the issue of conveyed broken hub location (DFD) in DTNs. A hub is considered as broken when one of its sensors much of the time reports incorrect estimations. The distinguishing proof of such flawed hubs is vital to save correspondence assets and toprevent wrong estimations dirtying gauges given by the DTN. This distinguishing proof issue is very confounded in DTNs when cooperations are for the most part between sets of experiencing hubs. A large portion of the traditional DFD calculations are utilizing estimations of spatially-connected actual amounts gathered by numerous hubs to decide the

presence of anomalies and recognize the hubs delivering these exceptions. If there should be an occurrence of pairwise

communications, crisscross between estimations given by two unique hubs can in any case be distinguished, however recognizing straightforwardly which hub produces wrong estimations is unimaginable. This paper presents a completely disseminated and effectively implementable calculation to permit every hub of a DTN to decide if its own sensors are inadequate. We accept as in [9] that hubs don't know about the status (great or faulty) of their sensors, while their calculation and correspondence capacities stay fine, regardless of whether a portion of their sensors are deficient. The majority of the DTN's nodes are assumed to act rationally and to be interested in learning about their sensors' status. A few hubs, notwithstanding, might be making trouble, attempting to irritate the identification cycle. As in [9], [10], [11], [12], [13], a Nearby Exception Identification

Test (LODT) is thought to have the option to distinguish the presence of exceptions in a bunch of estimations, without fundamentally having the option to figure out which are the anomalies. This is a run of the mill circumstance when just pairwise connections are thought of, where estimations from sensors of just two hubs are looked at. The conventional LODT is portrayed by its probabilities of location and misleading problem. At the point when two hubs meet,

they trade their neighborhood estimations and use them to play out a similar LODT. Both nodes can improve their estimates of the state of their own sensors with the assistance of the LODT results. When, for a given hub, the extent of gatherings duringwhich the LODT recommends the presence of exceptions is bigger than some edge, this hub concludes its sensors might be damaged. In this instance, it stops talking. Likewise, it communicates no more its estimations to its neighbors, yet continues to gather estimations from hubs met and refreshes the gauge of the situation with its sensors. It might then have the potential chance to change its gauge and convey once more. Albeit the LODT considered here are those of [9], this work varies fundamentally from [9] because of the correspondence states of DTNs, which require a very surprising DFD calculation. The examination of the properties of the calculation is additionally very surprising. Markov models and techniques derived from control theory and population dynamics are utilized in this study to demonstrate that the proposed DFD algorithm's behavior can be described using these approaches. More inside and out, the conviction of every hub about the situation with its

sensors is quantized. The advancement of these quantized convictions are then displayed to follow two Markov chains. A continuoustime estimate of the development of the extent of hubs with comparable convictions is then determined. Adequate circumstances on the choice boundaries to guarantee the presence and uniqueness of a balance of the DFD calculation are then given. Upper and lower bounds of the detection rate, or the proportion of nodes that have successfully identified their sensors as defective, and the false alarm rate, or the proportion of nodes that believe their good sensors are in fact defective, are also derived from the LODT's characteristics. The effect of getting out of hand hubs, attempting to annoy the aftereffects of the DFD calculation, is additionally considered. The DFD algorithm's parameters can be selected in accordance with the guidelines provided by these results.

## 2.LITERATURE SURVEY

### 1) TC-Aloha: A novel access scheme for wireless networks with transmit-only nodes

**AUTHORS:** L. Galluccio, G. Morabito, and S. Palazzo,

In the recent past several network scenarios have emerged where transmit-only nodes - i.e., nodes without receiving capabilities - are deployed. Such nodes cannot perform carrier sensing and cannot be synchronized. Therefore, they have to apply an Aloha-like medium access control. However, it is well known that Aloha achieves low good put due to the possibility to incur in collisions, and this results in poor energy efficiency too. In order to achieve better performance, in this paper a scheme called Timing-Channel Aloha (TC-Aloha) is introduced which exploits the timing channel. The timing channel is the logical communication channel established between a transmitter and a receiver in which the information is transferred by means of the timing of events. Another feature of TC-Aloha is that it enables multiple transmissions of the same information to improve the communication reliability. In this paper the TC-Aloha scheme is described in detail and an analytical framework is derived for the evaluation of its performance. The numerical results assess the advantages of TC-Aloha over traditional solutions.

### 2) Efficiency analysis of jamming-based countermeasures against malicious timing channel in tactical communications

**AUTHORS:** S. D'Oro, L. Galluccio, G. Morabito, and S. Palazzo

A covert channel is a communication channel that creates a capability to transfer information between entities that are not supposed to communicate. A relevant instance of covert channels is represented by timing channels, where information is encoded in timing between events. Timing channels may result very critical in tactical scenarios where even malicious nodes can communicate in an undisclosed way. Jamming is commonly used to disrupt this kind of threatening wireless covert communications. However jamming, to be effective, should guarantee limited energy consumption. In this paper, an analysis of energy-constrained jamming systems used to attack malicious timing channels is presented. Continuous and reactive jamming systems are discussed in terms of their effect on the achievable covert channel capacity and jammer energy consumption. Also, a simple experimental set up is illustrated and used to identify proper operating points where jamming against malicious timing channels is effective while achieving limited energy consumption.

**3) Jamming sensor networks: Attack and defense strategies**

**AUTHORS:** W. Xu, K. Ma, W. Trappe, and Y. Zhang

Wireless sensor networks are built upon a shared medium that makes it easy for adversaries to conduct radio interference, or jamming, attacks that effectively cause a denial of service of either transmission or reception functionalities. These attacks can easily be accomplished by an adversary by either bypassing MAC-layer protocols or emitting a radio signal targeted at jamming a particular channel. In this article we survey different jamming attacks that may be employed against a sensor network. In order to cope with the problem of jamming, we discuss a two-phase strategy involving the diagnosis of the attack, followed by a suitable defense strategy. We highlight the challenges associated with detecting jamming. To cope with jamming, we propose two different but complementary approaches. One approach is to simply retreat from the interferer which may be accomplished by either spectral evasion (channel surfing) or spatial evasion (spatial retreats). The second approach aims to compete more actively with the interferer by adjusting resources, such as power levels and communication coding, to achieve communication in the presence of the jammer.

**3.PROPOSED SYSTEM**

This study proposes a fully distributed approach that enables each DTN node to

use LODT done during the node meeting to assess the state of its own sensors. The evolution of the fraction of nodes with a particular belief in their status is taken into consideration when analysing the DFD algorithm.

### 3.1 IMPLEMENTATION

**Service Provider**

In this module, the Service Provider browses the required file, initializes nodes with digital signature and uploads to the end user (node a, node b, node c, node d, node e, node f) via Router.

**Router**

The Router is responsible for forwarding the data file in shortest distance to the destination; the Router consists of Group of nodes, the each and every node (n1, n2, n3,n4,n5,n6,n7,n8,n8,n10,n11,n12, n13) consist of Bandwidth and Digital Signature. If router had found any malicious or traffic node in the router then it forwards to the IDS Manager. In Router we can assign the Sleeping time for the nodes and can view the node details with their tags Node Name, Sender IP, Injected data, Digital Signature, Sleeping time and status.

**End User**

In this module, the End user can receive the data file from the Service Provider which is sent via Router, if malicious or traffic node is found in the router then it never forwards to the end user to filter the content and adds to the attacker profile.

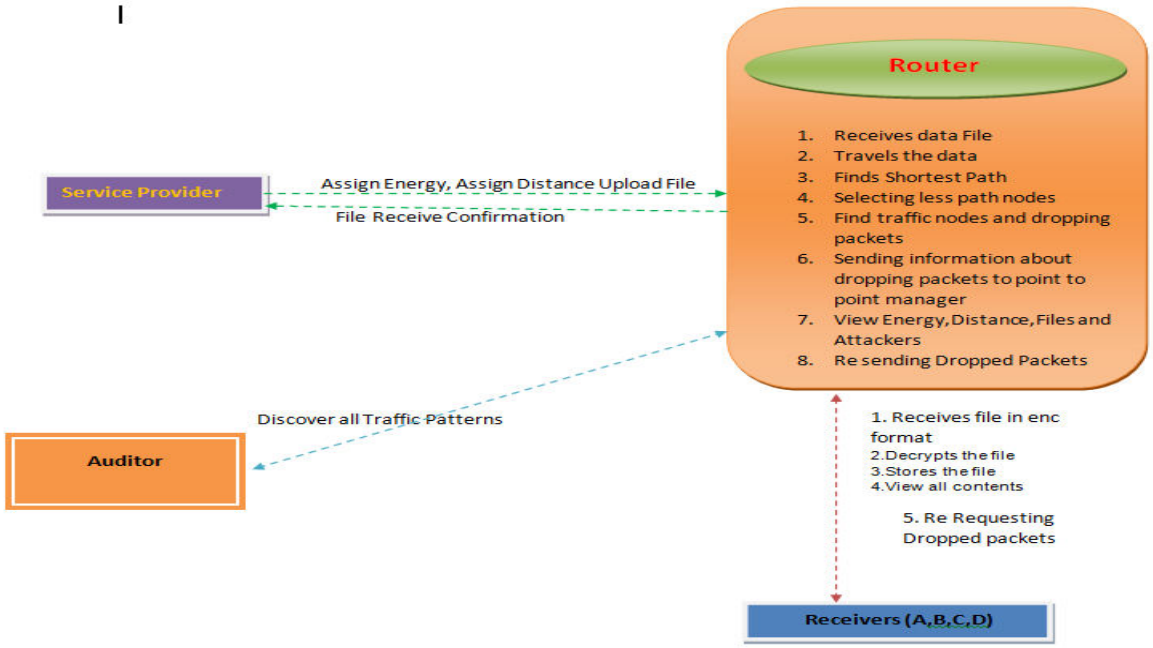
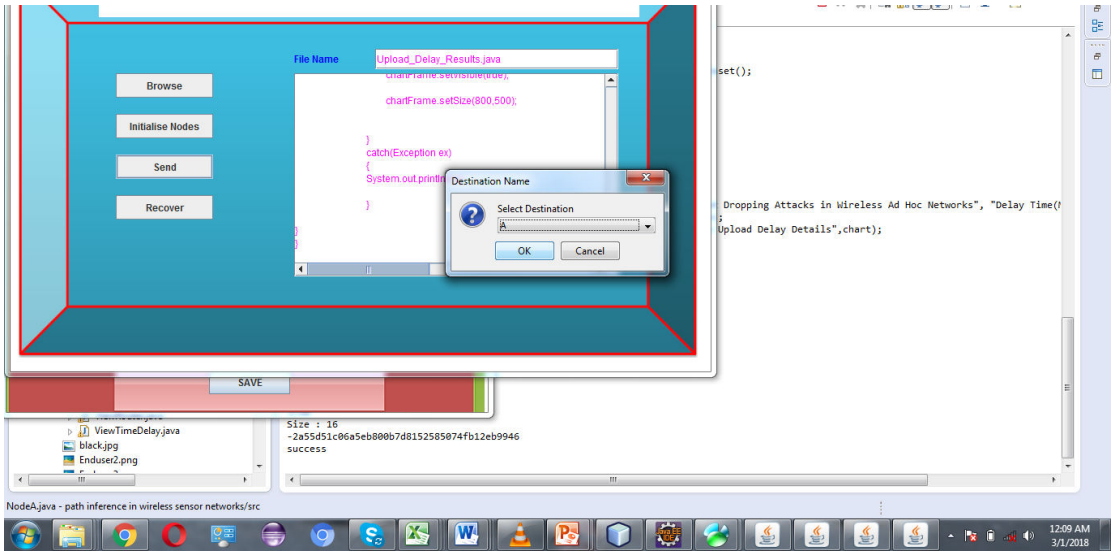
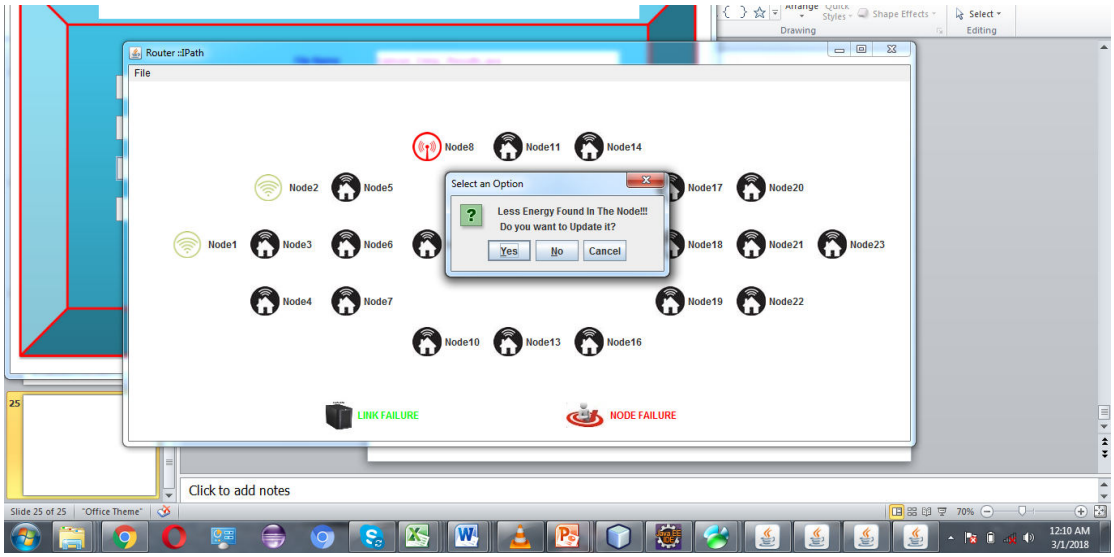
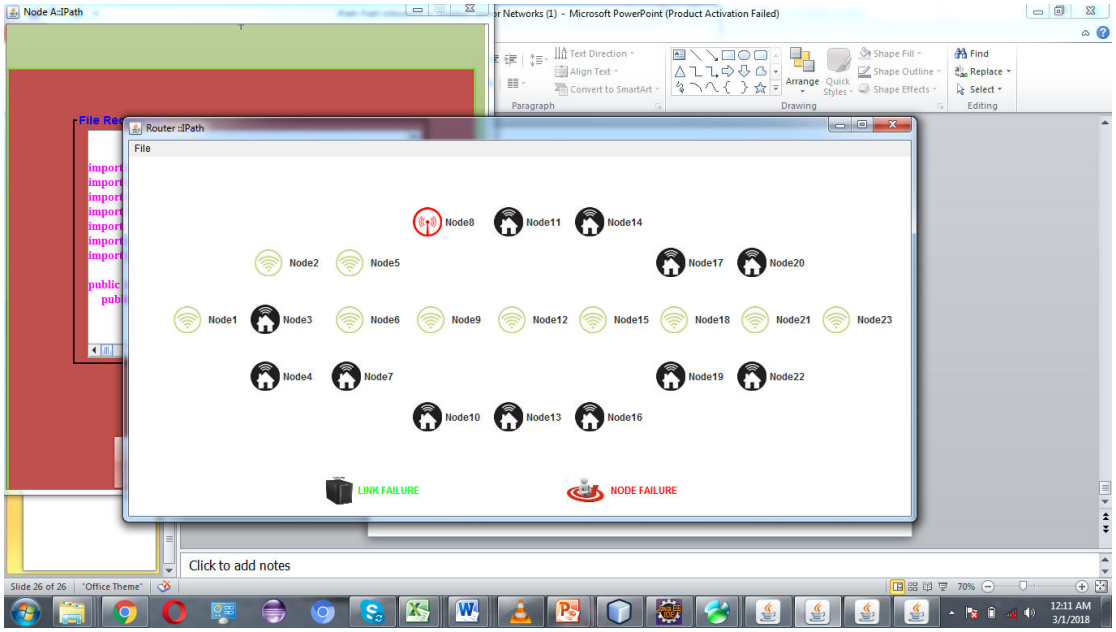


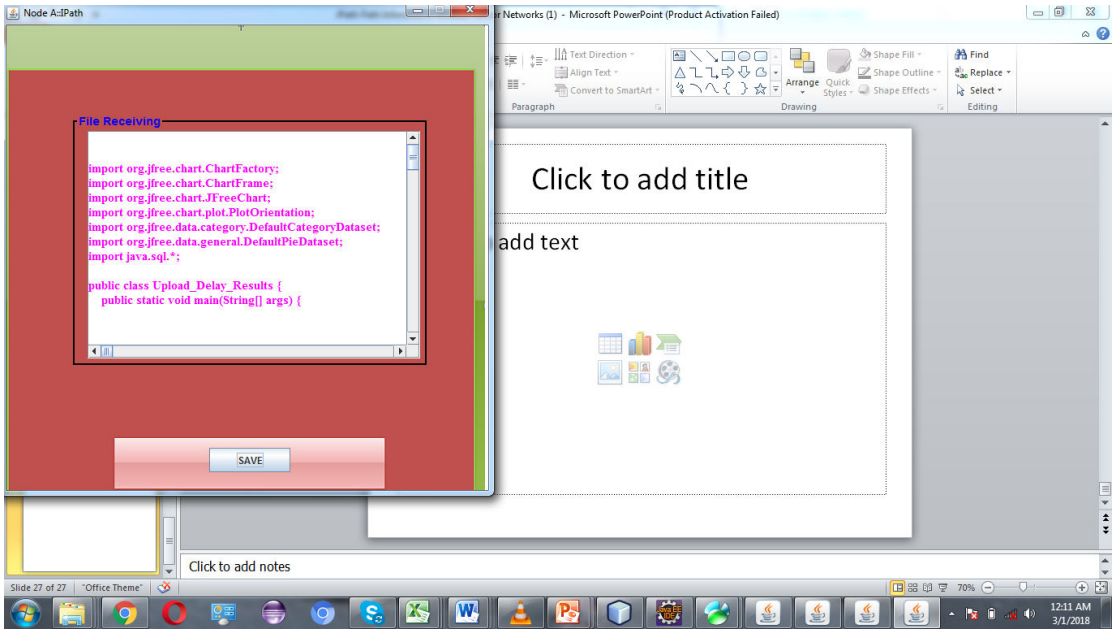
**Fig 1:Architecture**

## 4.RESULTS AND DISCUSSION






## 5.CONCLUSION

This work offers a completely distributed approach that enables every DTN node to use LODT, or local on-device tracking, to estimate the state of its own sensors during node meetings. A Markov model of the evolution of the proportion of nodes with a certain belief in their status is taken into consideration when analysing the DFD algorithm. The evolution of the proportions of the nodes in various states is then approximated by a series of

ordinary differential equations that are derived using this model. An equilibrium's existence and uniqueness are examined. It's interesting to note that the equilibrium proportions have a binomial distribution.

The approximations of these node proportions at equilibrium offer guidance on how to select the DFD algorithm's decision parameter appropriately. Databases containing traces of inter-contact time instants, a Brownian motion model, and a jump motion model are all taken into consideration in the simulations. The outcomes demonstrate a strong theoretical fit.The inter-contact rate and the percentage of nodes with faulty sensors (p1) determine how quickly the DFD algorithm converges. However, in equilibrium, p1 does not significantly affect the non-detection and false alarm rates, demonstrating the approach's resilience even when a large number of defective nodes are present. The robustness of the suggested DFD algorithm is demonstrated by the consideration of the impact of the existence of misbehaving nodes.

## REFERENCES

[1] M. Ceriotti *et al.*, "Monitoring heritage buildings with wireless sensor networks: The Torre Aquila deployment," in *Proc. IPSN*, 2009, pp. 277–288.

[2] L. Mo *et al.*, "Canopy closure estimates with GreenOrbs: Sustainable sensing in the forest," in *Proc. SenSys*, 2009, pp. 99–112.

[3] X. Mao *et al.*, "CitySee: Urban CO2 monitoring with sensors," in *Proc. IEEE INFOCOM*, 2012, pp. 1611–1619.

[4] O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, and P. Levis, "Collection tree protocol," in *Proc. SenSys*, 2009, pp. 1–14.

[5] D. S. J. D. Couto, D. Aguayo, J. Bicket, and R. Morris, "A highthroughput path metric for multi-hop wireless routing," in *Proc. MobiCom*, 2003, pp. 134–146.

[6] Z. Li, M. Li, J. Wang, and Z. Cao, "Ubiquitous data collection for mobile users in wireless sensor networks," in *Proc. IEEE INFOCOM*, 2011, pp. 2246–2254.

[7] X. Lu, D. Dong, Y. Liu, X. Liao, and L. Shanshan, "PathZip: Packet path tracing in wireless sensor networks," in *Proc. IEEE MASS*, 2012, pp. 380–388.

[8] M. Keller, J. Beutel, and L. Thiele, "How was your journey? Uncovering routing dynamics in deployed sensor networks with multi-hop network

tomography," in *Proc. SenSys*, 2012, pp. 15–28.

[9] Y. Yang, Y. Xu, X. Li, and C. Chen, "A loss inference algorithm for wireless sensor networks to improve data reliability of digital ecosystems.," *IEEE Trans. Ind. Electron.*, vol. 58, no. 6, pp. 2126–2137, Jun. 2011.

[10] Y. Liu, K. Liu, and M. Li, "Passive diagnosis for wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 18, no. 4, pp. 1132–1144, Aug. 2010.

[11] W. Dong, Y. Liu, Y. He, T. Zhu, and C. Chen, "Measurement and analysis on the packet delivery performance in a large-scale sensor network," *IEEE/ACM Trans. Netw.*, 2013, to be published.

[12] J. Wang, W. Dong, Z. Cao, and Y. Liu, "On the delay performance analysis in a large-scale wireless sensor network," in *Proc. IEEE RTSS*, 2012, pp. 305–314.

[13] Y. Liang and R. Liu, "Routing topology inference for wireless sensor networks," *Comput. Commun. Rev.*, vol. 43, no. 2, pp. 21–28, 2013.

[14] Y. Gao *et al.*, "Domo: Passive per-packet delay tomography in wireless ad-hoc networks," in *Proc. IEEE ICDCS*, 2014, pp. 419–428.

[15] M. Lee, S. Goldberg, R. R. Kompella, and G. Varghese, "Fine-grained latency and loss measurements in the presence of reordering," in *Proc. ACM SIGMETRICS*, 2011, pp. 329–340.

[16] Y. Shavitt and U. Weinsberg, "Quantifying the importance of vantage points distribution in internet topology measurements," in *Proc. IEEE INFOCOM*, 2009, pp. 792–800.

[17] M. Latapy, C. Magnien, and F. Oudraogo, "A radar for the internet," in *Proc. IEEE ICDMW*, 2008, pp. 901–908.

[18] I. Cunha, R. Teixeira, D. Veitch, and C. Diot, "Predicting and tracking internet path changes," in *Proc. SIGCOMM*, 2011, pp. 122–133.

[19] A. D. Jaggard, S. Kopparty, V. Ramachandran, and R. N. Wright, "The design space of probing algorithms for network-performance measurement," in *Proc. SIGMETRICS*, 2013, pp. 105–116.

[20] L. Ma, T. He, K. K. Leung, A. Swami, and D. Towsley, "Identifiability of link metrics based on end-to-end path measurements," in *Proc. IMC*, 2013, pp. 391–404.

[21] Y. Gao *et al.*, "Pathfinder: Robust path reconstruction in large scale sensor networks with lossy links," in *Proc. IEEE ICNP*, 2013, pp. 1–10.

[22] A. Woo, T. Tong, and D. Culler, "Taming the underlying challenges of reliable multihop routing in sensor networks," in *Proc. SenSys*, 2003, pp. 14–27.

[23] Y. Gao *et al.*, "iPath: Path inference in wireless sensor networks," Tech. Rep., 2014 [Online]. Available: http://www.emnets.org/pub/ gaoyi/tech-ipath.pdf

[24] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," in *Proc. IPSN*, 2008, pp. 245–256.

[25] V. Handziski, A. Köpke, A. Willig, and A. Wolisz, "TWIST: A scalable and reconfigurable testbed for wireless indoor experiments with sensor networks," in *Proc. REALMAN*, 2006, pp. 63–70.

**Author Profiles**

**Mr.VENKATARADHAKRISHNAMURTY**

He was Completed his Masters ofTechnology In ComputerScience and Engineering. He is dedicated to teaching filed from the last 19 years . Currently Working as an Associate Professor in the Department of CSE at ASCET(AUTONOMOUS), Gudur, Tirupathi (DT).His areas of interest include, Data Mining,Cloud Computing and Machine Learning.

**A.LAKSHMI SUPRIYA** is pursuing MCA from Audisankara institute of Technology (AUTONOMOUS), Gudur, Affiliated to JNTUA in 2024. Andhra Pradesh, India.