iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** V **Month of publication:** May 2016

DOI:

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Data Integrity and Delay Differentiated Routing (IDDR) Services in Wireless Sensor Networks (WSN's)

Konda. Hari Krishna[1], Dr. Tapas Kumar[2], Dr. Y. Suresh Babu[3]
[1]*Ph.D -Research Scholar- Lingaya's university & Assistant Professor, Dept. Of Computer Science & Engineering, Bharat Institute of Engineering and Technology*
[2]*Professor & Dean and H.O.D, Dept. Of Computer Science & Engineering, Lingaya's University, Faridabad,*
[3]*Professor, P.G Dept of Computer Science, JKC College, Guntur*

Abstract--Applications running on the same Wireless Sensor Network (WSN) platform usually have different Quality of Service (QoS) requirements. Two basic requirements are low delay and high data integrity. However, in most situations, these two requirements cannot be satisfied simultaneously. In this paper, based on the concept of potential in physics, we propose IDDR, a multi-path dynamic routing algorithm, to resolve this conflict. By constructing a virtual hybrid potential field, IDDR separates packets of applications with different QoS requirements according to the weight assigned to each packet, and routes them towards the sink through different paths to improve the data fidelity for integrity-sensitive applications as well as reduce the end-to-end delay for delay-sensitive ones. Using the Lyapunov drift technique, we prove that IDDR is stable. Simulation results demonstrate that IDDR provides data integrity and delay differentiated services.
Key Words: IDDR, QoS, Data Integrity, delay differentiated services, Dynamic routing, IDS, WSN'S, potential field.

I. INTRODUCTION

WSNS, which are used to sense the physical world, will play an important role in the next generation networks. Due to the diversity and complexity of applications running over WSNs, the QoS guarantee in such networks gains increasing attention in the research community.

As a part of an information infrastructure, WSNs should be able to support various applications over the same platform. Different applications might have different QoS requirements. For instance, in a fire monitoring application, the event of a fire alarm should be reported to the sink as soon as possible. On the other hand, some applications require most of their packets to successfully arrive at the sink irrespective of when they arrive. For example, in habitat monitoring applications, the arrival of packets is allowed to have a delay, but the sink should receive most of the packets. WSNs have two basic QoS requirements: low delay and high data integrity, leading to what are called delay sensitive applications and high-integrity applications, respectively. Generally, in a network with light load, both requirements can be readily satisfied. However, a heavily loaded network will suffer congestion, which increases the end-to-end delay.

This work aims to simultaneously improve the fidelity for high-integrity applications and decrease the end-to-end delay for delay-sensitive ones, even when the network is congested. We borrow the concept of potential field from the discipline of physics and design a novel potential based routing algorithm, which is called integrity and delay differentiated routing (IDDR). IDDR is able to provide the following two functions:

A. Improve Fidelity For High-Integrity Task Is To Find These Idle And/Or Under Loaded Applications

The basic idea is to find as much buffer space as possible from the idle and/or under-loaded paths to cache the excessive packets that might be dropped on the shortest path. Therefore, the first task is to find these idle and/or under loaded paths, then the second task is to cache the packets efficiently for subsequent transmission. IDDR constructs a potential field according to the depth1 and queue length information to find the under-utilized paths. The packets with high integrity requirement will be forwarded to the next hop with smaller queue length. A mechanism called Implicit Hop-by-Hop Rate Control is designed to make packet caching more efficient.

B. Decrease End-To-End Delay For Delay-Sensitive Applications

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Each application is assigned a weight, which represents the degree of sensitivity to the delay. Through building local dynamic potential fields with different slopes according to the weight values carried by packets, IDDR allows the packets with larger weight to choose shorter paths. In addition, IDDR also employs the priority queue to further decrease the queuing delay of delay sensitive packets. IDDR inherently avoids the conflict between high integrity and low delay: the high-integrity packets are cached on the under loaded paths along which packets will suffer large end-to-end delay because of more hops, and the delay-sensitive packets travel along shorter paths to approach the sink as soon as possible. Using the Lyapunov drift theory, we prove that IDDR is stable. Furthermore, the results of a series of simulations conducted on the TOSSIM platform demonstrate the efficiency and feasibility of the IDDR scheme.

II. OBJECTIVES

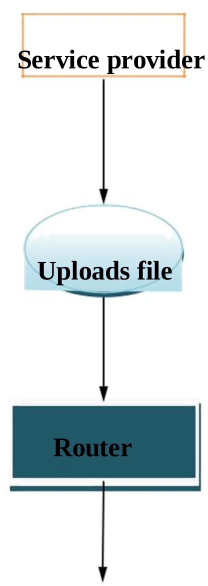
The basic idea is to find as much buffer space as possible from the idle and/or under-loaded paths to cache the excessive packets that might be dropped on the shortest path. Therefore, the first paths, then the second task is to cache the packets efficiently for subsequent transmission. IDDR constructs a potential field according to the depth1 and queue length information to find the under-utilized paths. The packets with high integrity requirement will be forwarded to the next hop with smaller queue length. A mechanism called Implicit Hop-by-Hop Rate Control is designed to make packet caching more efficient. Each application is assigned a weight, which represents the degree of sensitivity to the delay. Through building local dynamic potential fields with different slopes according to the weight values carried by packets, IDDR allows the packets with larger weight to choose shorter paths. In addition, IDDR also employs the priority queue to further decrease the queuing delay of delay sensitive packets.

IDDR inherently avoids the conflict between high integrity and low delay: the high-integrity packets are cached on the under loaded paths along which packets will suffer large end-to-end delay because of more hops, and the delay-sensitive packets travel along shorter paths to approach the sink as soon as possible. Using the Lyapunov drift theory, we prove that IDDR is stable. Furthermore, the results of a series of simulations conducted on the TOSSIM platform demonstrate the efficiency and feasibility of the IDDR scheme.

III. RELATED WORK

Most QoS provisioning protocols proposed for traditional ad hoc networks have large overhead caused by end-to-end path discovery and resource reservation. Thus, they are not suitable for resource-constrained WSNs. Some mechanisms have been designed to provide QoS services specifically for WSNs. Here we mainly focus on the metrics of delay and reliability.

IV. IMPLEMENTATION



Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering
Technology (IJRASET)

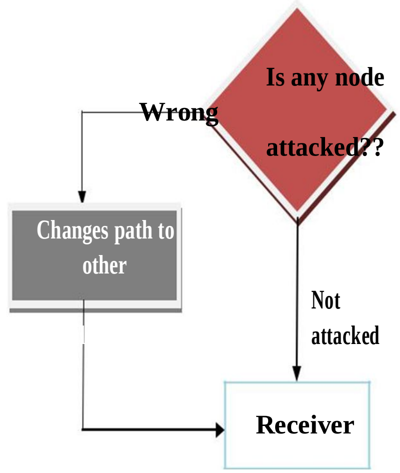


FIG: 1. System Architecture

A. Service Provider

In this module, the service provider will browse the data file, initialize the router nodes and then send to the particular receivers. Service provider will send their data file to router and router will select smallest distance path and send to particular receiver.

B. Router

The Router manages a multiple networks to provide data storage service. In network n-number of nodes are present (n1, n2, n3, n4, n5…). In a router service provider can view node details and attacked nodes. Service provider will send their data file to router and router will select smallest distance path and send to particular receiver. If any attacker is found in a node then router will connect to another node and send to particular user.

C. IDS Manager

In this module, the IDS Controller consists of two phases. If Integrity or Malicious Data is occurs in router then IDS controller is activated. In a first phase DNS packets, Net flow, Traffic filter and Fine-grained IDS client detection are present. Aim is that detecting all hosts within the monitored network that engage in IDS communications. We analyze raw traffic collected at the edge of the monitored network and apply a pre-filtering step to discard network flows that are unlikely to be generated by IDS applications. We then analyze the remaining traffic and extract a number of statistical features to identify flows generated by IDS clients. In the second phase, Coarse-grained IDS Integrity or Malicious Data detection, Fine-grained IDS client detection and Integrity or Malicious Data are present; our system analyzes the traffic generated by the IDS clients and classifies them into either *legitimate* IDS clients or IDS *Integrity or Malicious Data.*

D. Receiver (End User)

In this module, the receiver can receive the data file from the router. Service provider will send data file to router and router will send to particular receiver. The receivers receive the file by without changing the File Contents. Users may receive particular data files within the network only.

E. Attacker

Attacker is one who is injecting malicious data to the corresponding node and also attacker will change the bandwidth of the particular node. The attacker can inject fake bandwidth to the particular node. After attacking the nodes, bandwidth will changed in a router.

V. ALGORITHMS

Design of IDDR Algorithm Procedure of IDDR Consider a WSN with different high-integrity or delay-sensitive applications. Let c be the identifier of different applications. In summary, the main procedure of the IDDR algorithm at node i work as follows: 1. if the queue at node i is not empty, then aðcÞ ¼ a þ packet weight of p 0xff is computed for packet p at the head of the queue. 2. Let Wi;

bðtÞ¼ fðQiðtÞ þ aðcÞ DiðtÞÞðQbðtÞ þ aðcÞ Db ðtÞÞg. Select the next hop b¼ argmaxb2ViðtÞ; QjðtÞ6¼1Wi; bðtÞ. 3. Node i send packet p to node b. Go to (1). 3.4.2 Construction of Depth Potential Field The depth potential field is important because it provides the basic routing function. It is constructed based on the depth value of each node. At the beginning, the depth values of all the nodes are initialized to 0xff, except that the default depth of the sink is 0. The sink first sends a depth update message, the nodes one hop away from the sink obtain their own depth by adding 1 to the depth value in the update message and then send new update messages with their own depth values. Similarly, all the other nodes can obtain their own depth by receiving update messages from their neighbors who already know the depth value. Multiple sinks may exist in large scale WSNs. According to the procedure of the depth potential field construction, these sinks will periodically broadcast their update messages of depth. The nodes receive these update messages, compare the different depth values from different sinks, and then choose the nearest sink as its destination.

If the smallest depth value is not unique, the node can choose one of them randomly. Actually, when multiple sinks exist in a large scale WSN, IDDR will naturally partition the whole networks into sub regions managed by different sinks. Therefore, IDDR can work in large scale WSNs with multiple sinks. 3.4.3 Signaling. Each node requires the depth and queue length of its neighbors to make forwarding decisions. How often to update the depth and queue length between neighbors is quite important since too small period leads to much overhead while too large period leads to imprecise information.

IDDR defines a Maximum Update Interval (MUI) and a Least Update Interval (LUI) between two successive update messages. MUI is always larger than LUI. The update messages should be sent between a LUI and a MUI at least once. If no message is received from a neighbor during two MUIs intervals, this neighbor will be considered dead, and IDDR will recalculate the depth and other related values. An update message will be sent. The Slope of the potential field. The solid line represents the longitudinal section of depth potential field; the solid dots on the horizontal axis are nodes; the short vertical bars over the dots denote the normalized queue length of these nodes.

When any one of the following events occurs: (1) MUI timer expires. If the elapsed time since sending the last update message exceeds the MUI, a new update message will be sent immediately no matter whether the depth or queue length has changed. (2) Queue length variation exceeds a certain threshold. If the queue length of a node has varied 10 percent compared with that in the last successful update message and the elapsed time exceeds the LUI since the last update message. (3) Depth changes. If the depth of a node has changed, and the elapsed time exceeds the LUI since the last successful update message.

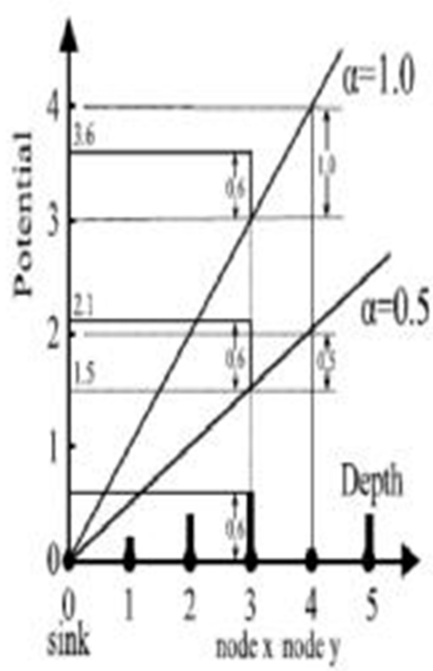


Fig: 2. Sink & Potential Graph

Volume 4 Issue V, May 2016
ISSN: 2321-9653

In a under-utilized WSN, the queue length is very small, the hybrid potential field is governed by the depth potential field. IDDR performs like the shortest path algorithm, that is, a node always chooses one neighbor with lower depth as its next hop. However, in a over-utilized WSN, the shortest paths are likely be full of packets. Therefore, new coming packets will be driven out of the shortest paths to find other available resource. If a node knows the queue length information of its neighbors, it can forward packets to the underloaded neighbors to stand against possible dropping. The following two propositions explain how IDDR reaches this goal.

Proposition 1. *Denote the depth of node v as d. Let S denote the neighbors of node v with the same depth, that is, $S = \{x|D_x(t) = d, x \in \Omega_v(t)\}$ and L denote the neighbors of node v with smaller depth, that is, $L = \{x|D_x(t) = d-1, x \in \Omega_v(t)\}$. Let $l \in L$ be the node with the minimal queue length in L. If node $s \in S$ has the minimum queue length in S and satisfies that $Q_s(t) < Q_l(t) - \alpha$, then node v will choose node s rather than node l as the next hop at time t.*

Proof. If node v does not choose node l as its parent, it will not choose any other nodes in L since node l has the minimal queue length and all the nodes in L have the same depth. The potential values at nodes, v, l and s, are:

$$V_v^m(t) = \alpha d + Q_v(t), \tag{5}$$

$$V_l^m(t) = \alpha(d-1) + Q_l(t), \tag{6}$$

$$V_s^m(t) = \alpha d + Q_s(t). \tag{7}$$

We can derive the force values at node v as follows:

$$F_{v \to l}^m(t) = \alpha + (Q_v(t) - Q_l(t)), \tag{8}$$

$$F_{v \to s}^m(t) = (Q_v(t) - Q_s(t)). \tag{9}$$

On the other hand, we can rewrite $Q_s(t) < Q_l(t) - \alpha$ as

$$(Q_v(t) - Q_s(t)) > \alpha + (Q_v(t) - Q_l(t)). \tag{10}$$

Hence, we can readily have $F_{v \to s}^m(t) > F_{v \to l}^m(t)$. According to the potential field model, node v will choose s as its next hop rather than l, which means that the packets from node v will be forwarded to the neighbors at the same depth since they have more available buffer space to cache packets. □

VI. RESULT

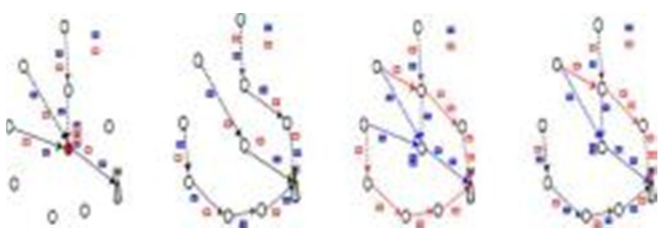


Fig 3(a) Action of SPT. (b) Action of multipath router. (c) Action of IDDR. (d) IDDR with hotspot.

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

VII. CONCLUSION

In this paper, a dynamic multipath routing algorithm IDDR is proposed based on the concept of potential in physics to satisfy the two different QoS requirements, high data fidelity and low end-to-end delay, over the same WSN simultaneously. The IDDR algorithm is proved stable using the Lyapunov drift theory. Moreover, the experiment results on a small test bed and the simulation results on TOSSIM demonstrate that IDDR can significantly improve the throughput of the high-integrity applications and decrease the end-to-end delay of delay sensitive applications through scattering different packets from different applications spatially and temporally. IDDR can also provide good scalability because only local information is required, which simplifies the implementation. In addition, IDDR has acceptable communication overhead.

REFERENCES

[1] P. Levis, N. Lee, M. Welsh, and D. Culler, “TOSSIM: Accurate and scalable simulation of entire Tiny OS applications,” in Proc. 1st Int. Conf. Embedded Networked Sensor Syst., 2003, pp. 126–137.
[2] T. Chen, J. Tsai, and M. Gerla, “QoS routing performance in multi hop multimedia wireless networks,” in Proc. IEEE Int. Conf. Universal Personal Commun, 1997, pp. 557–561.
[3] R. Sivakumar, P. Sinha, and V. Bharghavan, “CEDAR: Core extraction distributed ad hoc routing algorithm,” IEEE J. Selected Areas Commun., vol. 17, no. 8, pp. 1454–1465, Aug. 1999.
[4] S. Chen and K. Nahrstedt, “Distributed quality-of-service routing in ad hoc networks,” IEEE J. Selected Areas Commun., vol. 17, no. 8, pp. 1488–1505, Aug. 1999.
[5] B. Hughes and V. Cahill, “Achieving real-time guarantees in mobile ad hoc wireless networks,” in Proc. IEEE Real-Time Syst- 2003.
[6] E. Felemban, C.-G. Lee, and E. Ekici, “MMSPEED: Multipath multi-speed protocol for QoS guarantee of reliability and timeliness in wireless sensor networks,” IEEE Trans. Mobile Compute, vol. 5, no. 6, pp. 738–754, Jun. 2003.
[7] C. Lu, B. Blum, T. Abdelzaher, J. Stankovic, and T. He, “RAP: A real-time communication architecture for large-scale wireless sensor networks,” in Proc. IEEE 8th Real-Time Embedded Technol. Appl. Symp., 2002, pp. 55– 66.
[8] M. Caccamo, L. Zhang, L. Sha, and G. Buttazzo, “An implicit prioritized access protocol for wireless sensor networks,” in Proc. IEEE Real-Time Syst. Symp., 2002, pp. 39–48.
[9] T. He, J. Stankovic, C. Lu, and T. Abdelzaher, “SPEED: A stateless protocol for real-time communication in sensor networks,” in Proc. IEEE 23rd Int. Conf. Distrib. Compute. Syst., 2003, pp. 46–55.
[10] P. T. A. Quang and D.-S. Kim, “Enhancing real-time delivery of gradient routing for industrial wireless sensor networks,” IEEE Trans. Ind. Inform., vol. 8, no. 1, pp. 61–68, Feb. 2012.
[11] S. Bhatnagar, B. Deb, and B. Nath, “Service differentiation in sensor networks,” in Proc. Int. Symp. Wireless Pers. Multimedia Commun, 2001.
[12] B. Deb, S. Bhatnagar, and B. Nath, “Rein Form: Reliable information forwarding using multiple paths in sensor networks,” in Proc. IEEE Intl Conf. Local Compute. Netw. 2003, pp. 406– 415.
[13] M. Radi, B. Dezfouli, K. A. Bakar, S. A. Razak, and M. A. Nematbakhsh, “Interference-aware multipath routing protocol for QoS improvement in event-driven wireless sensor networks,” Tsinghua Sci. Technol., vol. 16, no. 5, pp. 475–490, 2011.
[14] J. Ben-Othman and B. Yahya, “Energy efficient and QoS based routing protocol for wireless sensor networks,” J. Parallel Distrib. Compute, vol. 70, no. 8, pp. 849–857, 2010.
[15] M. Razzaque, M. M. Alam, M. MAMUN-OR-RASHID, and C. S. Hong, “Multi-constrained QoS geographic routing for Heterogeneous traffic in sensor networks, ieice transactions on communications,” IEICE Trans. Commun., vol. 91B, no. 8, pp. 2589–2601, 2008.
[16] D. Djenouri and I. Balasingham, “Traffic-differentiation-based modular QoS localized routing for wireless sensor networks,” IEEE Trans. Mobile Compute, vol. 10, no. 6, pp. 797– 809, June 2010.
[17] A. Basu, A. Lin, and S. Ramanathan, “Routing using potentials: A dynamic traffic-aware routing algorithm,” in Proc. Conf. Appl., Technol., Architectures, Protocols Compute. Commun, 2003, pp. 37–48.
[18] C.-Y. Wan, S. B. Eisenman, and A. T. Campbell, “CODA: Congestion detection and avoidance in sensor networks,” in Proc. 1st Int. Conf. Embedded Netw. Sensor Syst., 2003, pp. 266–279.
[19] L. Georgiadis, M. J. Neely and L. Tassiulas, “Resource allocation and cross-layer control in wireless networks,” Found. Trends Netw, vol. 1, no. 1, pp. 1–144, 2006.
[20] A. Papadoulos and J. A. Mccann, “Towards the design of an energy-efficient, location-aware routing protocol for mobile, adhoc sensor networks,” in Proc. Int. Workshop Database Expert Syst. Appl., 2004, pp. 705–709.

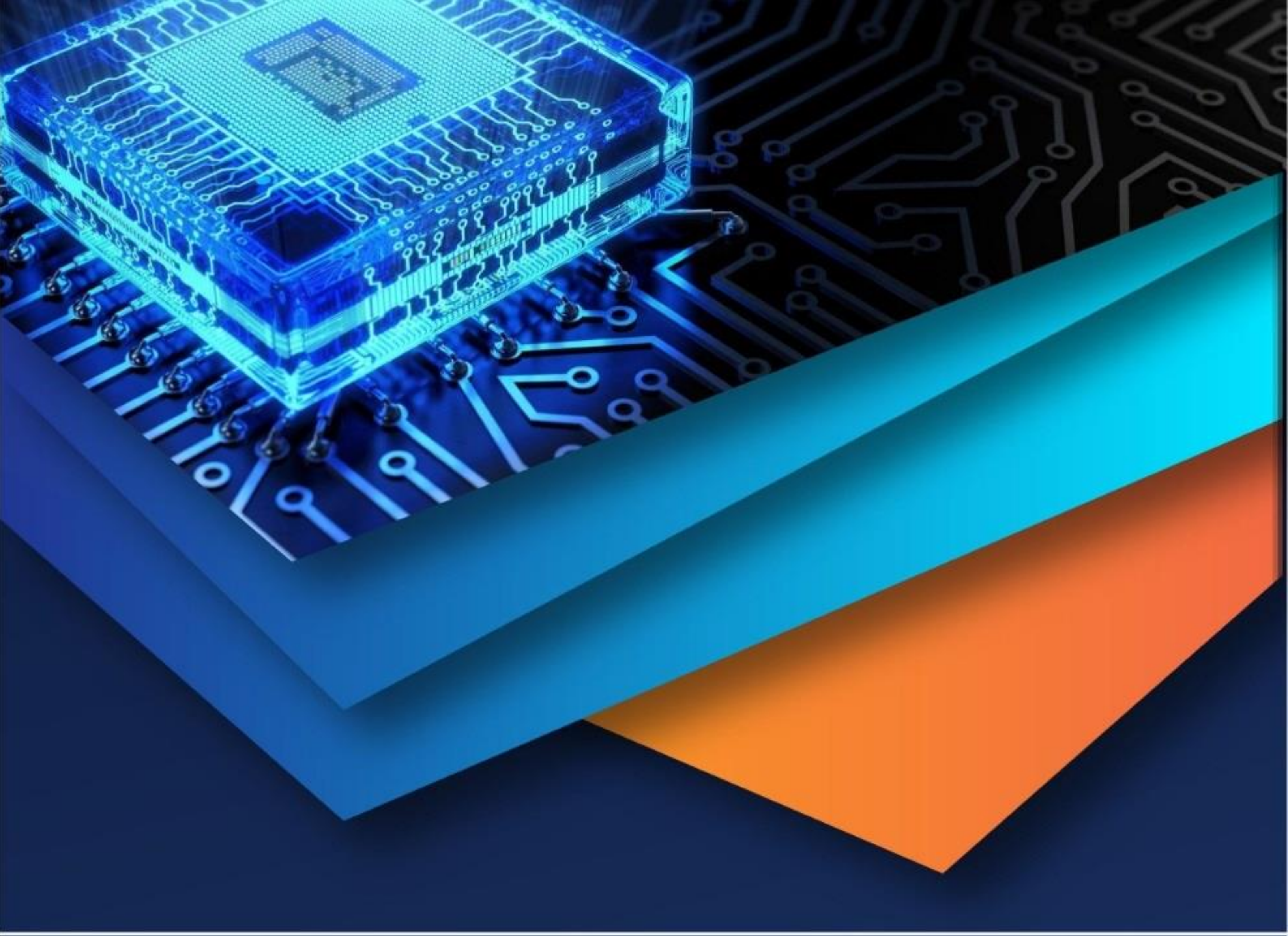
INFORMATION ABOUT AUTHORS

1. KONDA. HARI KRISHNA received his M.TECH in computer science from Jawaharlal Nehru Technological University, Kakinada & A.P and pursuing Ph.D in LINGAYA's University, Faridabad. He is working as an Assistant Professor in Bharat Institute of Engineering & Technology in Dept. of Computer Science & Engineering. He published 18 Research Papers in Various International Journals of Reputed and His Research Area is Mining of applications in Wireless Sensor Networks. He is a good researcher & who has worked mostly on Sensor networks, Ad hoc Networks, Network security and Data mining.

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Dr. TAPAS KUMAR, Working as a Professor, Dean & H.O.D in School of Computer Science & Engineering, Lingaya's University, Faridabad. He holds a Doctorate in Computer Science & Engineering. He has more than experience of 15 years in Academics & Administration. He has published various Research papers in various National & International Journals of Reputed.

Dr. Y. SURESH BABU, Working as a Professor in Dept of Computer Science, JKC COLLEGE, GUNTUR. He holds a Doctorate in Computer Science & Engg, Image processing as specialization with a combined experience of 23 years in Academics & Administration. He has published nearly 45 research papers in various National and International Journals of reputed**.**



10.22214/IJRASET

INDEX COPERNICUS
45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL
IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY