IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

Volume 13, Issue 5, May 2024

Impact Factor: 8.317

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.317|| A Monthly Peer Reviewed & Referred Journal |

||Volume 13, Issue 5, May 2024||

|DOI:10.15662/IJAREEIE.2024.1305058|

A New Methods for Secure and Low Latency Transmission in Industrial WSN

C. Jaya Priya[1], C R ajaNandhini[2]

PG Student, Department of Electronics and Communication Engineering, Periyar Maniammai Institute of Science and Technology, Vallam, Thanjavur, Tamilnadu, India

Assistant Professor, Department of Electronics and Communication Engineering, Periyar Maniammai Institute of Science and Technology, Vallam, Thanjavur, Tamilnadu, India.

ABSTRACT: Wireless sensor networks (WSNs) present unique challenges for protocol design, necessitating unconventional approaches. To achieve a long network lifetime while maintaining low device complexity and energy consumption, a balanced approach is necessary. Communication and signal/data processing capabilities must be identified. Over the past decade, there has been significant research, standardization, and corporate investment in this subject. This survey study provides an overview of wireless sensor network (WSN) technology, applications, standards, design characteristics, and evolution. The article discusses and highlights design ideas for certain applications, including environmental monitoring, and includes a case study of a real-world implementation. Trends and potential evolutions are tracked. The IEEE 802.15.4 technology is emphasized, as it enables numerous WSN applications. Performance characteristics of 802.15.4-based networks vary based on network size and data type transmitted between nodes. Examples are provided.

I. INTRODUCTION

Industrial wireless sensor networks (IWSNs) are expected to be employed in severe locations where radio transmissions are influenced by random noise and channel fading, resulting in packet mistakes that can impair production, equipment, and workers. To ensure deterministic real-time communication in industrial automation, IWSNs must have high reliability and low latency. A typical strategy to enhance link reliability is to use an automatic repeat request (ARQ) mechanism (a retransmission procedure), while another option is to use forward error correction (FEC) schemes, which reduce the bit error rate and hence the frequency of retransmissions.

ARQ is utilized in the majority of wireless systems to deal with erroneous packets. Still, given unfavorable channel conditions, it has been demonstrated that ARQ cannot satisfy the stringent latency requirements. The worst-case scenario is that the sender fails to transmit the data despite attempting the maximum retransmission times allowed by the protocol. Consider a network with numerous sensor nodes operating in this environment. The hard channel could cause a large number of retransmissions to occur at the same time. The bandwidth resources will be temporarily exhausted because too many nodes attempt to transmit data at the same time. Measurements reveal that transmission breakdown not only adds delay to industrial applications, but it can also cause network congestion.

One solution to this problem is to use forward error correction code. In an FEC code, more parity bits are included to the main message to recover damaged bits caused by the busy wireless channel. FEC has been studied for WSN in prior publications, however it is based on energy usage rather than memory size or processing time limits. It should be noted that including FEC into IWSN can raise energy usage, however this is still insignificant when considering other processing expenses.

In relation to energy usage, availability and reliability are far more significant. Severe congestion or missed deadlines in the wireless sensor network will stop the applications, which may result in economic loss or major safety issues. In this work, we look at how FEC codes can improve IWSN reliability and minimize latency. Because the absence of access to the "silicon" makes using FEC codes in the physical layer impractical, we offer a method for applying FEC codes at the MAC layer instead. Our suggested approach divides the whole MAC layer packet, except for the FCS field, into groups and encodes it using systematic FEC codes. The extra redundancy from each encoded group is then gathered and put in a new FEC field at the tail of the payload, along with a new flag in the header indicating FEC code operation.

The reasoning behind this proposed solution is that when a sensor node gets a message, It is able to verify the packet using the FCS checksum. If no bit errors are identified, the node can filter the packet based on the header without decoding it. We also look into the execution times of various FEC codes to ensure that we are not violating the stringent timing restrictions for acknowledgments. As a result, we benchmarked many unique FEC codes such as Bose-Choudhary-Hocquenhem (BCH), Reed Solomon (RS), and Golay code on an embedded system to verify that the computation duration of FEC exceeds the execution time limit and that the FEC code uses an appropriate amount of memory.

The MAC procedure produces adequate information that can be accessed without connecting with adjacent. Latency and energy usage can be further decreased while remaining reliable. Certain routing information-based tactics can be utilized during the routing phase to improve the probability of handshake success in MAC. In routing, the sender can select next-hops with fewer rivals. To acquire neighbor information, extra topology update packets are required. Unlike control packets, these topology update packets can be broadcast when the channel is idle, minimizing the impact on transmission.

II. REVIEW OF LITERATURE

A reliable RSS-based routing protocol for industrial wireless sensor networks
Author: **Kan Yu. Mikael Gidlund**
Year: **2022**

A high level of reliability and instantaneous operation are the primary research challenges for Industrial Wireless Sensor Networks (IWSNs). Existing routing protocols used in IWSNs are either overly complex or fail to meet the demanding requirements. In this research, we offer a routing strategy based on Received Signal Strength that is both dependable and versatile. Our proposed method ensures a smooth transition in the event of a topology change and can be used in a variety of industrial contexts. According to the simulation results, our method beats standard routing protocols in terms of reliability and latency. Finally, the suggested technique is demonstrated to achieve much improved dependability in scenarios with obstructions while avoiding installation issues when compared to a location-based flooding approach. Therefore, our proposed strategy is thought to be more appropriate for IWSNs.

A co-design-based reliable low-latency and energy-efficient transmission protocol for uwsns
Author**: Xiaohui Wei**
Year: **2022**
In recent times, underwater wireless sensor networks (UWSNs) have been regarded as a powerful method for a variety of applications. But acoustic communications in UWSNs cause significant QoS difficulties for time-critical tasks. Furthermore, extra control packets and numerous copies throughout the data transmission process exacerbate the problem. To address these issues, we present a reliable low-latency and energy-efficient transmission protocol for dense 3D underwater wireless sensor networks to improve UWSN QoS.First, our forwarding-set routing technique will significantly minimize the amount of handshakes in the MAC process while ensuring dependability. Second, using MAC process information, network-update messages can be utilized to substitute control packages when selecting a route using mobility prediction. Simulation findings reveal that the suggested protocol has much higher reliability, lower latency, and energy usage in comparison to existing transmission protocols for a dense underwater wireless sensor network.

Enhancing graph routing algorithm of industrial wireless sensor networks using the covariance-matrix adaptation
Author**:NoufAlharbi** Year: **2022**

The rise of the Industrial Internet of Things (IIoT) has pushed the use of Industrial Wireless Sensor Networks (IWSNs) for a variety of applications. Effective communication in such applications necessitates shorter end-to-end transmission times, more balanced energy use, and improved communication dependability. Graph routing, the primary routing approach in IWSNs, has a substantial impact on achieving successful communication while meeting these standards. Graph routing techniques use the first-route available strategy and path redundancy to send data packets from a source sensor node to the gateway. However, this strategy can have an impact on end-to-end transmission time by causing conflicts between transmissions utilizing a similar sensor node and promoting uneven energy use due to centralized administration.

Deep q-learning based resource allocation in industrial wireless networks for urllc
Author:**NoufAlharbi** Year: **2022**

URLLC is one of the probable solutions supplied by 5G technology for an industrial wireless network.. Furthermore, reinforcement learning is gaining traction because of its ability to learn from both observed and unobserved results. Industrial wireless nodes (IWNs) may fluctuate dynamically due to internal or external causes, necessitating the depreciation of the non-essential reconfiguration of network resource allocation. To address this problem, MANETdeep Q-learning (DQL)-based resource allocation algorithms based on the learning of experienced trade-offs and interdependencies in IWN are proposed. The presented findings show that the algorithm can identify the most effective ways for improving resource allocation. Furthermore, DQL underscores the need for improved control in order to have ultra-reliable and low-latency IWN.

Cross-layer analysis of error control in wireless sensor networks
Author:**Mehmet C. Vuran**
Year: **2006**
Severe energy limits, and hence low power transmission requirements, highlight the importance of energy efficient and, preferably, cross-layer error control systems in wireless sensor networks (WSN). This work presents a cross-layer methodology for analyzing error control strategies in WSNs, focusing on the implications of multi-hop routing and the broadcast aspect of the wireless channel. More particular, the cross-layer implications of routing, media access, and physical layers are examined. This analysis allows for a full comparison of forward error correction (FEC) and automatic repeat request (ARQ) in WSNs.

In a multi-hop system, this improvement can be realized by lowering the transmit power (transmit power control) or by building longer hops (hop length extension), which can be accomplished using channel-aware routing algorithms. Our research indicates that for specific FEC codes, the hop length extension minimizes overall energy usage and complete latency when tested against a target PER compared to ARQ. Thus, FEC codes can be considered an essential candidate for delay-sensitive traffic in WSNs. On the other hand, transmit power regulation saves significant amounts of energy but increases delay. Furthermore, at different end-to-end distances and goal PER values, ARQ outperforms FEC codes.

Survey of routing attacks and countermeasures in mobile ad hoc network
Author: **Abdelaziz Amara Korba** Year: **2016**
Mobile Ad Hoc Mobile ad hoc networks (MANETs) are made up of self-organizing mobile nodes that have dynamic topologies and no fixed infrastructure. These networks are especially vulnerable to security concerns due to their dynamic ad hoc character, in which unknown devices create spontaneous relationships with one another. In recent years, significant efforts have been made to build secure and resilient routing protocols, with security methods proposed to address these security challenges. We explore all routing dangers that may impact the functioning of routing protocols, which might be egoistic actions or malicious attacks, along with defenses against these attacks. We have grouped them into three categories in an organized manner: cryptographic solutions, intrusion detection systems, and trust management and reputation solutions.

An efficient heuristic candidate selection algorithm for opportunistic routing in wireless multihop networks
Author: **Amir Darehshoorzadeh**
Year: **2016**
Opportunistic Routing (OR) is a new type of routing system that selects the next-hop forwarder on the fly. It makes use of the broadcast aspect of the wireless medium. OR increases wireless transmission reliability by selecting a pool of candidates for forwarding packets to their destinations. In this paper, we present a new heuristic and a fast candidate selection technique based on the link delivery probability from one node to the candidate node. We will call it the Heuristic Candidate Selection Algorithm Based on Optimum Delivery Probability (HU-COP).

. HU-COP selects candidates through linkages that have delivery probability near to ideal. Furthermore, the performance of HU-COP is extremely similar to the findings of the most efficient algorithm in a variety of cases. Furthermore, HU-COP identifies the sets of candidates significantly faster than the other methods.

Local cooperative relay for opportunistic data forwarding in mobile ad-hoc networks
Author:**Zehua Wang**
Year: **2016**
Since the publication of the seminal paper ExOR, opportunistic data forwarding has received increasing attention in the wireless network research community. However, as far as we know, all present opportunistic data forwarding uses

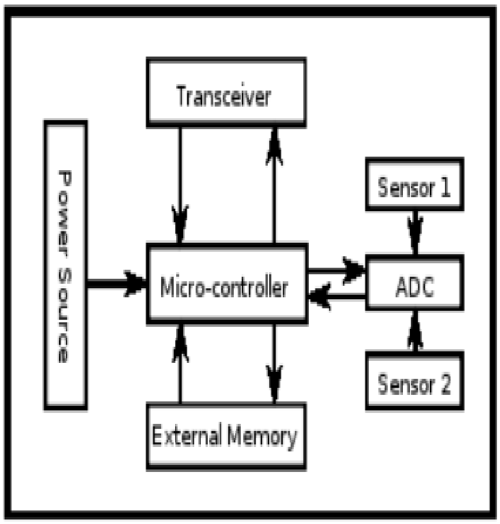
nodes from the forwarder list throughout the forwarding process. In reality, even if a node is not specified as a forwarder in the forwarder list, but it is on the path from source node to destination node, and it successfully overhears certain packets by chance, the node can be used in the opportunistic data forwarding process. This research proposes a local cooperative relay for opportunistic data forwarding in mobile ad-hoc networks.

. In general, we have three contributions in this paper: 1) we open more nodes to participate in the opportunistic data forwarding even though the nodes are not included in the forwarder list; 2) we propose a procedure to select the best local relay node, namely the helper-node, from many candidates but require no inner communication between them; and 3) the helper-node is selected just when it is needed, and such real-time selection can tolerate and bridge vulnerable links.

Privacy-preserving and truthful detection of packet dropping attacks in wireless ad hoc networks
Author:**Tao Shu**
Year**: 2014**

In a multi-hop wireless ad hoc network, the loss of packets are frequently due to malicious packets falling or connection problems.. In this research, we examine a series of packet losses in the network to determine whether the losses are caused only by link problems or by a combination of link errors and malicious drops. We are particularly interested in the insider-attack scenario, in which malevolent nodes along the route use their understanding of the communication context to choose delete a limited number of packets crucial to network performance. To improve quality of detection, we suggest exploiting correlations between missing packets. Furthermore, to ensure that these correlations are calculated accurately, we create a homomorphic linear authenticator (HLA)-based public auditing architecture that allows the detector to validate the accuracy of packet loss information reported by nodes. This design protects privacy, prevents collusion, and has low communication and storage overheads. To reduce the computation cost of the baseline technique, a packet-block-based mechanism is developed, allowing one to trade detection accuracy for lower calculation complexity.

III. BLOCK DIAGRAM



Controller:

The controller is responsible for task execution, data processing, and controlling other sensor node components' operation. While microcontrollers are the most prevalent type of controller, others include general-purpose desktop microprocessors, digital signal processors, FPGAs, and ASICs. A microcontroller is commonly employed in many embedded systems, including sensor nodes, due to its low cost, versatility in connecting to other devices, ease of programming, and low power consumption.

Transceiver:

Sensor nodes frequently make use Of the ISM band, which provides free radio, spectrum allocation, and worldwide availability. Wireless transmission modalities include radio frequency (RF), optical communication (laser), and infrared. Lasers use less energy, but they require a clear line of sight and are sensitive to atmospheric conditions.

External memory:
The most energy-efficient types of memory are on-chip microcontroller memory and Flash memory.Off-chip RAM is rarely if ever used. Flash memories are employed for their low cost and large store capacity. Memory requirements vary greatly depending on the application. Memory is divided into two types based on its function of storage: user memory, which is used to store application-related or personal data, and program memory, which is used to program the device. If the device's identifying data exists, it is also stored in program memory.

Sensors:
Wireless sensor nodes use sensors to collect environmental data. They are hardware devices that respond in measurable ways to changes in physical conditions such as temperature or pressure. Sensors measure physical data about the parameter being monitored and have certain qualities such as accuracy, sensitivity, and so on. The continuous analog signal generated by the sensors is processed by an analog-to-digital converter and supplied to controllers for further processing. Sensors in WSN gather environmental factors and are used for data acquisition. Sensor signals are translated to electrical signals.

Radio nodes:
Radio Nodes receive and transmit sensor data to the WLAN access points. It includes a microcontroller, a transceiver, external memory, and a power supply.

WLAN:
It receives data sent wirelessly by the Radio nodes, typically via the internet.

IV. CONCLUSION

The mobile node works as an intermediary in the mobile network, connecting with other nodes and rejecting intrusion attempts. The malicious node operations result in packets being transmitted with higher-quality data loss. It was difficult to reject and identify harmful communication that should be transmitted further with a high packet loss rate and low attack detection efficiency. The approach proposed that enhanced improved data forwarding guards against intrusions that have previously detected selective forwarding on mobile nodes. To damage invaders, a routing network that restricts or eliminates packet sharing is required. To provide an example of an effective method, an upgraded relay node that is efficient does not lose packets and rejects the process. The construction route is efficient, and communication is essential.

REFERENCES

[1] T. Braun, M. Heissenbüttel, and T. Roth, “Performance of the beaconless routing protocol in realistic scenarios,” Ad Hoc Network, vol. 8, no. 1, pp. 96–107, 2010.
[2] T. Saaty, Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process, RWS Publications, 2001.
[3] Z. Wang, C. Li, and Y. Chen, “Local cooperative relay for opportunistic data forwarding in mobile ad-hoc networks,” in 2012 IEEE International Conference on Communications (ICC), pp. 5381–5386, Ottawa, ON, Canada, 2012.
[4] A. Darehshoorzadeh and L. Cerd’a-Alabern, “Candidate selection algorithms in opportunistic routing,” in Proceedings of the 5th ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks, pp. 48– 54, Bodrum, Turkey, 2010.
[5] M. Musolesi and C. Mascolo, “Car: context-aware adaptive routing for delay-tolerant mobile networks,” Mobile Computing, IEEE Transactions, vol. 8, no. 2, pp. 246–260, 2009.
[6] B. Karp and H. T. Kung, “Gpsr: greedy perimeter stateless routing for wireless networks,”in Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 243–254, Boston, Massachusetts, USA, 2000.
[7] A. K. Abdelaziz, M. Nafaa, and G. Salim, “Survey of routing attacks and countermeasures in mobile ad hoc networks,” in 2013 UKSim 15th International Conference on Computer Modelling and Simulation, pp. 693–698, Cambridge, UK, 2013.
[8] P. M. Jawandhiya, M. M. Ghonge, M. S. Dr, P. Ali, and J. S. Deshpande, “A survey of mobile ad hoc network attacks,” International Journal of Engineering Science and Technology, vol. 2, no. 9, pp. 4063–4407, 2010.

[9] S. Vhora, R. Patel, and N. Patel, “Rank base data routing (RBDR) scheme using AOMDV: a proposed scheme for packet drop attack detection and prevention in MANET,” in 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), pp. 1–5, Coimbatore, India, 2015.

[10] T. Shu and M. Krunz, “Privacy-preserving and truthful detection of packet dropping attacks in wireless ad hoc networks,” IEEE Transactions on Mobile Computing, vol. 14, no. 4, pp. 813–828, 2015.

[11] R. H. Morelos-Zaragoza, The Art of Error Correcting Coding, Second Edition, JOHN WILEY and SONS, LTD, 2006.

[12] J. Åkerberg, M. Gidlund, M. Bjorkman, Future research challenges in wireless sensor and actuator networks targeting industrial automation, ¨ to appear in IEEE 9th International Conference on Industrial Informatics (INDIN’11) (2011) 154 –159.

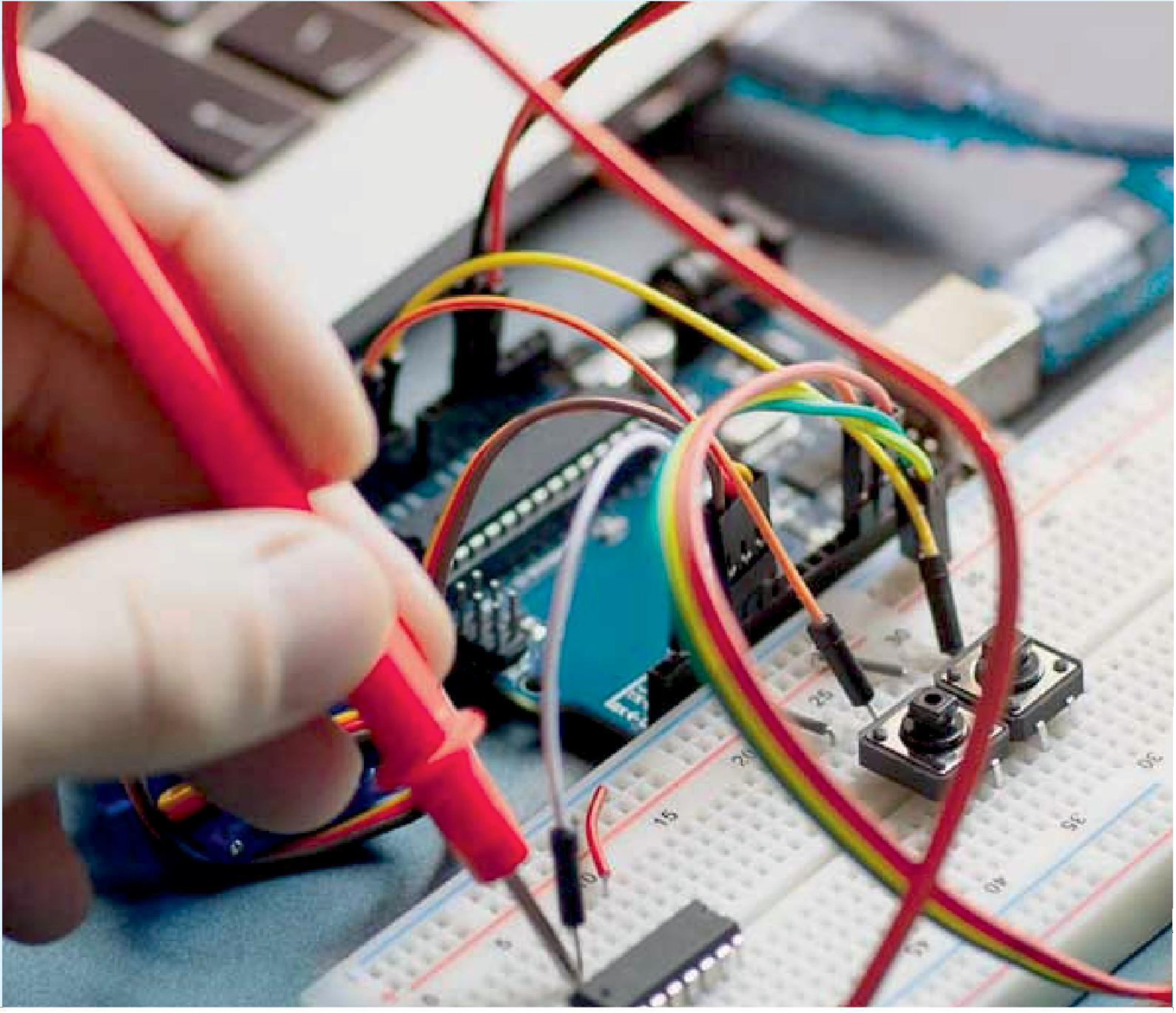
[13] J. Åkerberg, M. Gidlund, F. Reichenbach, M. Bjorkman, Measurements on an industrial wireless hart network supporting profisafe: A case ¨ study, to appear in IEEE Conference on Emerging Technologies and Factory Automation (ETFA’11) (2011) 1–8.

[14] S. Kim, R. Fonseca, D. Culler, Reliable transfer on wireless sensor networks, Sensor and Ad Hoc Communications and Networks, 2004 (2004) 449.

[15] L. Li, R. Maunder, B. Al-Hashimi, L. Hanzo, An energy-efficient error correction scheme for ieee 802.15.4 wireless sensor networks, Circuits and Systems II: Express Briefs, IEEE Transactions on 57 (3) (2010) 233 –237.

[16] M. Vuran, I. Akyildiz, Cross-layer analysis of error control in wireless sensor networks, Sensor and Ad Hoc Communications and Networks, 2006. SECON ’06. 2006 3rd Annual IEEE Communications Society on 2 (2006) 585 –594.

[17] A. Sikora, V. Groza, Coexistence of ieee802.15.4 with other systems in the 2.4 ghz-ism-band, Instrumentation and Measurement Technology Conference, 2005. IMTC 2005. Proceedings of the IEEE 3 (2005) 1786 –1791



International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

Scan to save the contact details

www.ijareeie.com