© 2019 IJSRSET | Volume 6 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology
DOI : 10.32628/IJSRSET

Review : Secure energy-efficient IoT based wireless sensor networks: Findings and Challenges

Dr. J. Keziya Rani[1], M. Sri Lakshmi[2]

[1]Assistant Professor, Department of Computer Science & Technology, S.K University, Anantapuramu, Andhra Pradesh, India

[2]Research Scholar, Department of Computer Science & Technology, S.K University, Anantapuramu, Andhra Pradesh, India

ABSTRACT

Wireless sensor networks (WSNs) have demonstrated research and developmental interests in numerous fields, like communication, agriculture, industry, smart health, monitoring, and surveillance. Sensor nodes are treated as smart devices and widely used to gather and forward sensed information. However, besides intrinsic constraints on sensor nodes, they are vulnerable to a variety of security threats. This paper reviews the findings and Research challenges on secure energy-efficient IoT based wireless sensor networks.

Keywords : Wireless Sensor Networks, Internet of Things, Sensor nodes, Security.

I. INTRODUCTION

In various domains, the technology of wireless sensor network (WSN) [1–3] has been used in an efficient way to improve network performances. The main reason to uses different sensors in the environmental field due to their manageable and easy configuration setup [4]. Additionally, the sensor nodes operate autonomously and construct the network infrastructure in an ad-hoc manner. In such infrastructure, nodes have not a stable network topology, and they can join the more suitable neighbor for data transmission based on some factors. The sensor nodes sense the observing data and forward towards BS with the help of some gateway and cluster heads. These cluster heads have a role of aggregating the received data packets and relay towards BS. The cluster heads effectively construct a single-hop or multi-hop path to BS and work as a focal point in entire data transmission.

Furthermore, the cluster heads store the received data in its memory and follow the store and forward mechanism. The end-users access the centralized BS via the Internet or different web-based applications to retrieve the required observing data. During data transmission, the deployed sensors can be static or mobile.

The static sensors are also referred to as non-adaptive and their constructed routing tables are fixed. While on the other hand, the routing tables of mobile sensors are dynamic and frequently updated when any change incurs in the network topology. The static routing solutions are more secure when compared to dynamic routing; however, the solutions that are based on the static algorithms are not appropriate for large regions and network scalability In recent years, the technology of IoT has been merged a lot with other fields to improved communication in terms of network throughput, resource utilization, and load distribution [7–9]. In IoT, many physical objects are attached to convert the information while using the

Internet. Moreover, the technology of WSN provides the foundation for IoT systems and supports in observing and forwarding the conditions for the physical environment. Devices in such IoT networks will typically operate based on battery power sources, and hence, energy efficiency is naturally of utmost importance in device management. Looking into a particular Wireless Sensor Network (WSN) domain, energy efficiency for battery operated sensor nodes and lifetime prolongment have been researching issues for so long [5, 6].

II. LITERATURE REVIEW

In the recent era, the technologies of WSN have been applied by different fields because of their low cost, easy deployment, and cost-effective environment [10,11]. In WSN, a large number of sensor nodes are scattered in observing the field to sense the needed data. All of the data are gathered and forwarded towards BS via single or multi-hop adopted data transmission paradigm for post-analysis.

In WSN [12–13], many researchers have proposed different clustering schemes that aimed to prolong network lifetime and efficient data transmission [14–15]. In such schemes, WSN divided into various regions, and each region has one cluster head, which aims to gather and forward the sensory information towards BS. Furthermore, most of the sensor nodes moved to sleep mode for prolonging network lifetime. Low energy adaptive cluster hierarchy (LEACH) was proposed by [16], aiming to introduce the concept of a cluster-based approach and improve energy efficiency as compared to traditional approaches. The role of the cluster head is randomly rotated and, accordingly, the LEACH protocol balances the energy consumption among the sensor nodes.

In [17], the authors proposed the analytic hierarchy process (AHP), which aims to centralize the process of cluster head selection mechanism. Residual energy, mobility, and distance towards cluster centroid are considered to be the main factors for the selection process of cluster heads. The proposed solution significantly improved network lifetime in the comparison of other solutions.

The authors in [18] proposed an energy-efficient k-means technique (EKMT) and determined the optimal cluster heads. The selected cluster heads are closer to the cluster's member as well as the BS. The proposed solution offers to decrease the communication distance among nodes and improve the network lifetime. However, the proposed solution is not efficient in an insecure and unrestricted space environment, as it is open to malicious extortions and might be harmful to sensors data.

Authors [19] proposed cluster head selection in wireless sensor networks while using a fuzzy environment. The proposed solution based on the fuzzy multiple attribute decision making (MADM) approach and uses residual energy, distance to BS, and the number of neighbor's factors for selecting the cluster heads.

A simulated network lifetime is prolonged than hierarchical agglomerative clustering (DHAC) [20] protocol under a homogeneous background. An improved chain-based clustering hierarchical routing (ICCHR) algorithm that is based on LEACH [21] consists of cluster formation, cluster head selection, chain formation, and data transmission phases The selection and distribution of cluster heads in the proposed protocol are non-optimal and they cause extra energy consumption. Based on simulation results, the proposed ICCHR algorithm decreases the ratio of energy consumption, evenly distributing the load among sensor nodes.

The authors in [22] proposed an optimized zone-based energy-efficient routing protocol for mobile sensor networks (OZEEP). The main aim of the proposed solution is to improve the network performance in terms of cluster formation and cluster head selection based on distance, density, mobility,

and energy factors. The proposed solution achieves balanced energy consumption and improved network lifetime; however, the evaluation of wireless links is missing in the proposed solution. Moreover, security measurements are also not taken into consideration, which results in frequent links and routing failures.

The authors [23] proposed the particle swarm optimization-energy efficient-based cluster head selection (PSO-ECHS) protocol, which prolongs network lifetime and network stability. In the proposed PSO-ECHS protocol, the cluster heads are selected using fitness function, which comprises residual energy, distance from sensor nodes to neighbors, and distance from sensor nodes to BS. The cluster heads are selected based on minimum fitness value and, afterwards, the cluster formation phase is initiated. All of the selected cluster heads announced their advertisement message and normal nodes joined them to formulate the clusters.

In [24], the authors proposed a secure user authentication and key agreement scheme while using WSN, which aims to monitor the agriculture domain securely. The proposed protocol is validated using Burrows-Abadi-Needham (BAN) logic, and the simulation results demonstrate better improvement in terms of security against malicious attacks. However, in most of the other existing works, the proposed solution also does not consider the performance of links in data transmission and leads to packets drop and latency ratio.

In the ambient trust sensor routing (ATSR) [25], the authors presented energy and trust-aware routing protocol. To detect malicious nodes, the presented solution proposes a distributed, secure routing protocol and evaluates the trust value of neighbors based on trust metrics. The ATSR protocol is feasible for large scale networks, as the decision is made by using local information of neighbors. However, this protocol incurs higher network traffic due to the Flooding of Route Request and Route Response Packets and Lead to Maximize Energy Consumption.

III. APPLICATIONS OF WSN WITH IoT

With the starting of this trend, WSN research focuses on network information processing and network technologies suitable for ad hoc environment and highly dynamic sensor nodes. Furthermore, advancement in technology also helped to reduce the size of sensor nodes as cost as well, resulting in emergent of many civil applications such as vehicular sensor network, environment monitoring and body sensors.

3.1.1 Military applications:

- Battlefield surveillance
- Monitoring friendly forces, ammunition and equipment
- Assessment of battle damage
- Biological, chemical and nuclear attack reconnaissance and detection

3.1.2 Environmental applications:

- Temperature, humidity sensing
- Forest fire detection
- Flood detection
- Environment biocomplexity mapping
- Agriculture irrigation

3.1.3 Health applications:

- Telemonitoring of human physiological data
- Heartbeat, pulse monitoring
- Drug administration

3.1.4 Other applications:

- Home automation
- Environmental control in office
- Vehicle tracking
- Noise level
- Presence of absence of certain kinds of objects

IV. CLASSIFICATIONS OF SENSOR NODES

4.1 Terrestrial WSN: sensor nodes deployed in a random or preplanned way in terrestrial WSN. Nodes can be arranged in grid placement in preplanned deployment. Different routing protocols, energy minimization technique can be applied in terrestrial WSN.

4.2 underground WSN: sensor nodes are positioned deep underground soil, mine or in cave to monitor the underground condition. In underground WSN deployment is difficult than terrestrial WSN as it involves careful planning. Mostly, battery recharging or replacement can not be implemented in this scenario.

4.3 Underwater WSN: sensor nodes can be deployed underwater for monitoring, exploring and disaster prevention. Such wireless nodes are expensive as compare to others and have minimal bandwidth for transmission. In underground WSN batteries almost cannot be replaced or recharged. Preplanning for deployment is also required.

4.4 Mobile WSN: sensor nodes are capable of moving in mobile WSN. Sensor nodes can also sense the physical environment and can-do self-configuration. These nodes provide effective connectivity and coverage. Mobile nature makes them enable to monitoring habitat, target tracking, and surveillance in military applications.

4.5 Multi-Media WSN: sensor nodes can store, retrieve and process multimedia data such as video and audio. High bandwidth, security, Qos, link quality and power required for multimedia WSN. Nodes can contain microphone, cameras and other sensors to observe the surrounding.

V. CHALLENGES AND ISSUES IN WSN WITH IoT

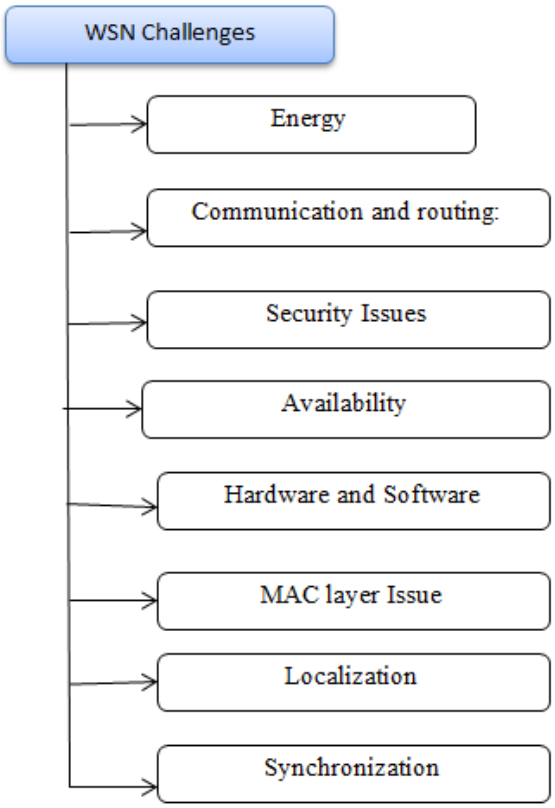

Figure 1. Challenges and Issues in WSN with IoT

5.1 Energy: sensors require energy or power backup to operate and process various operations. Energy management is main issues in WSN.

5.2 Communication and routing: communication with base station is very challenging to keep node alive for long period of time. Mostly, nodes only support small coverage for communication. Routing protocols, and deployment strategy directly affect the communication and overall performance for WSN.

Many routing protocols and algorithms are already developed for WSN that can be divided into seven categories. Each algorithm has its own merits and demerits. These algorithms can be used depending on the nature of the application.

- Location-based protocol
- Data-centric protocols
- Hierarchical protocols
- Mobility based protocols

- Multipath based protocols
- Heterogeneity based protocols
- QoS Based Protocols

5.3Security Issue: Security in a wireless sensor network is one of the critical issues. As in WSN data travel wirelessly through the air, so wireless signals are open to everyone; thus, anyone can monitor and participate as well, in communication. Mostly nodes in WSN operate in ISB band that is license-free. Security becomes very important in commercial and mostly military applications to prevent malicious attacks, Unnotarized access and denial of service DoS attacks [26]. Security requirements [27] or WSN can be divided as follow:

Data confidentiality: a major problem in the wireless operated network is that radio spectrum is an open medium and can easily be monitored by everyone. An attacker can sniff and interfere with the transmitted packet. The captured packet can be altered for misleading information.

Data authenticity: new misleading packet can be injected into communication between nodes by an attacker if he somehow knows the packet format defined in WSN protocol stack. Injected packet can carry misleading or incorrect information. in object tracking, environment monitoring application can be disturbed by injected incorrect information. to overcome this issue standard approach can be used in which authenticity maintained by use of message authentication code, signature, secret key, challenge-response, multi and broadcasting authentication.

Data integrity: owing to the instability of wireless channels, transmission errors are inherent in WSN. Due to many reason information travelling in electromagnetic signals can be changed for example signal fading, signal reflection, signal diffraction, scattering, and various kind of noise. This is the reason of wastage of transmission. Incorrect data needs to be retransmitted and it very expensive in WSN. The message integrity code can ensure data integrity.

5.4 Availability: availability of sensor nodes is essential to monitor critical zones. Owing to excess or unnecessary communication and computation sensor nodes can be run out of battery power. To make sure the availability of nodes energy-efficient routing algorithm and protocols need to be implemented.

5.5 Hardware and software issue: As sensor nodes reducing in size, a limited amount of resource like memory, processing speed and energy is also an issue for WSN. Typically, the sensor node has a microcontroller, sensor, transceiver, and power backup.

5.6 MAC Layer Issue: in wireless sensor network, a lot of energy wastage found at MAC layer during a collision, idle listening packet overhead, busty traffic.

5.7 Localization: Mostly, nodes are deployed randomly in real-world scenarios; it is challenging to manage and locate them in the absence of supporting infrastructure.

5.8 Time Synchronization: sensor nodes operated in the field independently, sometimes their local clocks not synchronized with other nodes that could be a reason for ambiguity and uncertainty of sensed data.

VI. FINDINGS

It is seen from the discussed studies that sensor nodes are minimal in terms of battery power, transmission, storage, and processing resources. Additionally, it is not possible to replace the components of the sensor nodes in dense and large regions. These low powered sensor nodes have a significant impact on the performance of the network in terms of delivery ratio and energy consumption.

Therefore, optimizing network lifetime with stable routing and data delivery performance are most of the important research challenges in WSN based applications. Additionally, the selection of cluster

heads performs a significant role to balance the load distribution and energy consumption in the WSN.

The cluster heads that are one hop away from BS exhaust their energy resource much quickly and lead to the energy hole issue, which degrades network throughput and increases the latency ratio. Moreover, it is observed from the existing work that most of the solution does not consider the strength of the signal in data routing, which significantly increases the packet drop ratio and instability in the network region. Accordingly, most of the energy power of sensor nodes is dissipated due to the selection of poor wireless carrier channels. It leads to frequent retransmissions of sensors' data.

Furthermore, end users obtained the information from the IoT based WSN while using the Internet, which is full of malicious actions, and network information can be disclosure to anonymous nodes. Therefore, data security is another crucial research aim for a WSN. to achieve network reliability and trustworthiness. Consequently, an energy-efficient and secure IoT based WSN framework must be layout and developed for smart agriculture to optimize network lifetime with reliable delivery performance to end-users. Besides, a reliable mechanism can increase the security of individual sensors and formulate realistic end-to-end routing paths. Therefore, the combined concept of energy efficiency with lightweight data security among the low power sensor nodes can improve the efficacy of the IoT-based WSN framework.

III. SUGGESTIONS

Several researchers have used the technology of WSN in various domains to sense environmental data. WSN has also played a vital role in the observation and management of agricultural land in terms of crops, climate, water usage, etc. However, there is a research scope to develop energy-efficient and secure IoT-Based WSN Framework for any environmental or other applications.

IV. CONCLUSION

One of the emerging networking standards that gap between the physical world and the cyber one is the Internet of Things. In the Internet of Things, smart objects communicate with each other, data are gathered, and individual requests of users are satisfied by different queried data. The development of efficient energy schemes for the IoT is a challenging issue as the IoT becomes more complicated due to its large scale the current techniques of wireless sensor networks cannot be applied directly to the IoT. The technology of wireless sensor networks performs a vital role in the development of various domains. This paper reviews several challenges and issues with secure energy-efficient IoT based wireless sensor networks. And also discuss the several Wireless sensor network applications and its challenges with further research scope.

V. REFERENCES

[1] Chen Dvir, A.; Ta, V.T.; Erlich, S.; Buttyan, L. STWSN: A novel secure distributed transport protocol for wireless sensor networks. Int. J. Commun. Syst. 2018, 31, e3827.

[2] Mehra, P.S.; Doja, M.N.; Alam, B. Fuzzy based enhanced cluster head selection (FBECS) for WSN. J. King Saud Univ.-Sci. 2018, 32, 390–401.

[3] Tripathi, A.; Gupta, H.P.; Dutta, T.; Mishra, R.; Shukla, K.K.; Jit, S. Coverage and connectivity in WSNs: A survey, research issues and challenges. IEEE Access 2018, 6, 26971–26992.

[4] Shahzad, M.K.; Cho, T.H. An energy-aware routing and filtering node (ERF) selection in CCEF to extend network lifetime in WSN. IETE J. Res. 2017, 63, 368–380.

[5] K.I. Kim, “Clustering Scheme for (m, k)-Firm Streams in Wireless Sensor Networks,” the

Journal of information and communication convergence engineering, vol.14, no. 2, pp. 84-88, 2016.

[6] Y.B. Cho, S.H. Lee and S.H. Woo, "An Adaptive Clustering Algorithm of Wireless Sensor Networks for Energy Efficiency", Journal of The Institute of Internet, Broadcasting and Communication (IIBC), vol. 17, no. 1, pp.99-106,2017.

[7] Khattak, H.A.; Ameer, Z.; Din, U.I.; Khan, M.K. Cross-layer design and optimization techniques in wireless multimedia sensor networks for smart cities. Comput. Sci. Inf. Syst. 2019, 16, 1–17.

[8] Din, I.U.; Guizani, M.; Hassan, S.; Kim, B.S.; Khan, M.K.; Atiquzzaman, M.; Ahmed, S.H. The Internet of Things: A review of enabled technologies and future challenges. IEEE Access 2018, 7, 7606–7640.

[9] Awan, K.A.; Din, I.U.; Almogren, A.; Guizani, M.; Altameem, A.; Jadoon, S.U. Robust trust–a pro-privacy robust distributed trust management mechanism for internet of things. IEEE Access 2019, 7, 62095–62106.

[10] Alaparthy, V.T.; Morgera, S.D. Multi-level intrusion detection system for wireless sensor networks based on immune theory. IEEE Access 2018, 6, 47364–47373.

[11] Rawat, P.; Singh, K.D.; Chaouchi, H.; Bonnin, J.M. Wireless sensor networks: A survey on recent developments and potential synergies. J. Supercomput. 2014, 68, 1–48.

[12] Yu, Y.; Liu, J. An Energy-Aware Routing Protocol with Small Overhead for Wireless Sensor Networks. In Proceedings of the International Conference on Data Mining and Big Data, Shanghai, China, 17–22 June 2018; Springer: Berlin/Heidelberg, Germany, 2018.

[13] Haseeb, K.; Islam, N.; Almogren, A.; Din, I.U. Intrusion Prevention Framework for Secure Routing in WSN-Based Mobile Internet of Things. IEEE Access 2019, 7, 185496–185505.

[14] Darabkh, K.A.; Albtoush, W.Y.; Jafar, I.F. Improved clustering algorithms for target tracking in wireless sensor networks. J. Supercomput. 2017, 73, 1952–1977.

[15] Zhu, C.; Wu, S.; Han, G.; Shu, L.; Wu, H. A tree-cluster-based data-gathering algorithm for industrial WSNs with a mobile sink. IEEE Access 2015, 3, 381–396.

[16] Heinzelman, W.R.; Chandrakasan, A.; Balakrishnan, H. Energy-efficient communication protocol for wireless microsensor networks. in System Sciences, 2000. In Proceedings of the 33rd Annual Hawaii International Conference, Maui, HI, USA, 7 January 2000; IEEE: Maui, HI, USA, 2000.

[17] Karaca, O.; Sokullu, R.; Prasad, N.R.; Prasad, R. Application oriented multi criteria optimization in WSNs using on AHP. Wirel. Pers. Commun. 2012, 65, 689–712.

[18] Jain, B.; Brar, G.; Malhotra, J. EKMT-k-means clustering algorithmic solution for low energy consumption for wireless sensor networks based on minimum mean distance from base station. In Networking Communication and Data Knowledge Engineering; Springer: Berlin/Heidelberg, Germany, 2018; pp. 113–123.

[19] Azad, P.; Sharma, V. Cluster head selection in wireless sensor networks under fuzzy environment. ISRN Sens. Netw. 2013, 2013, 1–8.

[20] Lung, C.H.; Zhou, C. Using hierarchical agglomerative clustering in wireless sensor networks: An energy-efficient and flexible approach. Ad. Hoc. Netw. 2010, 8, 3280–3344.

[21] Wu, H.; Zhu, H.; Zhang, L.; Song, Y. Energy Efficient Chain Based Routing Protocol for Orchard Wireless Sensor Network. J. Electr. Eng. Technol. 2019, 14, 2137–2146.

[22] Srivastava, J.R.; Sudarshan, T.S.B. A genetic fuzzy system based optimized zone based energy efficient routing protocol for mobile

sensor networks (OZEEP). Appl. Soft Comput. 2015, 37, 863–886.

[23] Rao, P.S.; Jana, P.K.; Banka, H. A particle swarm optimization based energy efficient cluster head selection algorithm for wireless sensor networks. Wirel. Netw. 2017, 23, 2005–2020.

[24] Ali, R.; Pal, A.K.; Kumari, S.; Karuppiah, M.; Conti, M. A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring. Future Gener. Comput. Syst. 2018, 84, 200–215.

[25] Darabkh, K.A.; Albtoush, W.Y.; Jafar, I.F. Improved clustering algorithms for target tracking in wireless sensor networks. J. Supercomput. 2017, 73, 1952–1977.

[26] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009 .

[27] BRORING, A. et al. New generation sensor web enablement. Sensors, 11, 2011, pp. 26522699. ISSN 1424-8220. Available from: doi:10.3390/s110302652

Cite this article as :

Dr. J. Keziya Rani, M. Sri Lakshmi, "Review : Secure energy-efficient IoT based wireless sensor networks: Findings and Challenges", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 6 Issue 2, pp. 698-705, March-April 2019.
Journal URL : http://ijsrset.com/IJSRSET207554