Journal of Advances in Science and Technology
Vol. 18, Issue No. 1, March-2021, ISSN 2230-9659

A Review on Routing Protocols for Security and Energy Efficiency in WSNs

Kulkarni-Shinde Bharat Pralhad[1*], Dr. C. Ram Singla[2], Dr. Sanjay B. Patil[3]

[1] Ph.D. Student, SunRise University, Alwar

[2] Guide, SunRise University, Alwar

[3] Co-guide, SCSCOE, Pune

Abstract – Wireless sensor networks (WSNs) have received a lot of interest recently. Because keeping track of things is so crucial, an increasing number of sensor networks are being set up via wireless connections. Despite their ubiquitous use, sensors pose a variety of infrastructural issues. Several research on wireless sensor networks are now being undertaken. Increasing the endurance of sensors has emerged as a prominent topic in research. Keep in mind that a sensor is a tiny electrical component with a limited power source. The battery or equivalent power source supplies the energy required by the device to execute its duties. Keeping the nodes charged and changed out may be difficult if they are spread apart. In addition to hardware problems, energy consumption is a crucial factor. Idle listening, rebroadcasting, overhearing, and overemitting all result in energy waste. Data may be collected from a large number of sensors that can be put everywhere, no matter how harsh or unforgiving the surroundings are, using Wireless Sensor Networks (WSNs). Due to the harsh environment and limited battery life span of battery-operated sensors, research and development of trustworthy, secure, and energy-efficient sensor network protocols is necessary. In wireless sensor networks, information exchange accounts for 70% of total energy consumption, making routing the most essential protocol in terms of energy utilisation (WSNs) (WSNs). As a result, energy-efficient routing algorithms must be developed in order to minimise network loads and extend the service life of current infrastructure. However, because of their application-specific character, the lack of a global solution scheme, and resource-limited sensors, creating information routing in WSNs creates considerable challenges. Because sensors are frequently placed in the least secure area, making them exposed to security threats and phishing, privacy and security are also critical problems in WSNs. Many security procedures are built into the systems of the various routing protocols already in use. In this brief essay, we will present an introduction of numerous routing protocols for wireless sensor networks, focusing on their fundamental operations and principles to illustrate how energy-efficient and secure they may be.

Keywords – Routing, WSN, Energy Efficiency and Security

----------X----------

INTRODUCTION

WSN, which stands for "Wireless sensor network," is a technology that has both civilian and military applications. These systems rarely make use of highly sensitive and individually tailored data, such as reports acquired from sensors placed in various parts of the body, to monitor the health of critical patients, where entire types of decision and prescription are selected based on information provided by sensors. There have been several developments in both methodology and algorithm, with trust-based algorithms providing advantages over more traditional approaches. Information at all system nodes may be verified for its authenticity and integrity using such methods. Congestion of data in the system is just one of the many complications that might arise during the implementation of trust-based solutions. See Figure1 for a breakdown of how WSNs are built.

The network's overall lifespan is drastically shortened, having a direct, negative impact on the data-gathering process as a knock-on effect. According to our findings, a secure and practical secure aware routing (RSAR) protocol may be developed. With this method, we can get over the obstacles we've hit thus far. As a first step, it assesses the reliability of each sensor node in a network.The conditional tug of war optimisation approach is used to determine the values of the outputs based on the optimum trust inference. The rate at which data travels from one node to another in a multi-hop network can be slowed with the aid of information aggregation, so that only the information

that is truly required is conveyed at the end of the chain. The suggested work achieves energy efficiency by conveying frequent and defective data from acquired data, which improves WSN lifespan by preserving its battery. By measuring trust characteristics, this method assists in identifying data assaults and reducing their impacts.

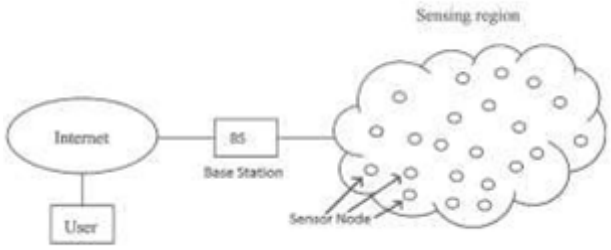

Figure 1: Architecture of WSN

As WSN technology evolves and expands, there is an increasing demand for more advanced security measures. Sensitive information and natural processes are conveyed and carried out by sensor networks in unattended environments; consequently, security issues must be addressed from the beginning of system design. The development of security procedures necessitates a thorough understanding of the capabilities and limits of each underlying technology.

Malicious nodes can create transmission distortions such as the Doppler effect and multi-path routing, hence WSNs must be designed to withstand attacks and malicious behaviour from individual nodes. If a node at a critical junction becomes malicious, the resulting interference at the destination could cause an error or cause the recipient to receive the same message multiple times, but the transmitting node would not be held accountable because the information would have been sent via a different path. Message distortion, impersonation, interference, message replay eavesdropping, and the revelation of sensitive information are all possible outcomes of an assault.

As a result, understanding trust-affected restrictions is essential for creating useful security mechanisms that accept and apply notions from modern security approaches. An RSAR protocol concept may be used to overcome these kinds of problems, which depend on the data aggregation model and the interference of optimum trust. Every sensor node uses a CTWO-based trust inference model for its computation of trust degree. Cluster-dependent data aggregation, which is energy efficient, is implemented for combining nodes with a good degree of trust, improving information forwarding by reducing attack contribution for future forwarding nodes in a system.

LITERATURE REVIEW

The upcoming research scenarios like security and environment of energy efficient routing in WSN were discussed in this part. Detailed information on these topics is provided in following subsections.

Energy efficient modelling WSN [1]- [3] —protocol restrict to meet transmited power with optimum node synchronization error [4] for any size of network. It is not realizable and becomes economically over burden to replace sensors as nodes are empowered by energy storage devices like batteries and expected to continuously function, Therefore vitality management is a primary problems related to WSN [5], [6]. Transmission depends on routing method as previous evaluations depicts that larger part of energy is utilised for in transmission [7]. Hence, it becomes compulsory to design and helps in formulating energy management guidelineto undisputedly save energy and improves lifespan of systems network. In [8] researches have suggested a novel algorithm depending on ACO to search for shortest path between static nodes of high level of energy.‖ However suggested model does not pass in proving in case of network of mobile and doesn‘t provides network parameter‘s theoretical analysis of systems.

In [9] routing of conventions gather data inWSN are presented. Nodes are intentionally orchestrated with the help of scattered bunch production mechanism. Variations in this convention is extended at large as channel delays as it has to pass through many sensors in reaching at base station. By actualizing one-sided discretionary strolling strategy such decline is overwhelmed. By rendezvous point based onsplittreetechniquesshortesttransmissionpath is determined from [10]. For multiple mobile sink topologies these approach has not been proved. Suggested directing techniques is unsuitable for static sink as its positions changes constantly [11]as loss of data can occurs due to invalid paths used for data transfer. For restricting vitality and network delay QBD Cconspireis presented In[12].Evenwith sufficient amount of sensors still, this method is confined to specific application. By increasing amount of sensors applied in systems of CoIS building of many mobile sink information breaking concept is achieved as this work is extended in [13].

There is a possibility of information interruption and node failure with densely deployed WSNs. To determine such failure of node using local split detection approach an attempt has been made in [14]. However suggested enhancement is not as predicted compared to existing techniques. In information sensitive WSN applications throughputis a vital factor. To study performance of network by successively rising number of nodes MRADC model is put forth in article [15]. Based on heterogeneous structure with many sinks behaviour of data assortmentisim proved by combining information [13] – [18]. By conveying versatile sink rather than nodes concept of portability is suggested in WSNs [19]. However, while implementing versatile sink is very much easy and simple to actualize, it becomes unfeasible for portable execution of data transfer. To investigate influence of various network

parametersin consumer network, depending on these EMCAand MECA algorithms are put forth in [20].

Khadije and Fatemeh et. al. [21] proposed an improvedRoutinginWirelessSensorNetworksusing Harmony Search Algorithm. This paper is concentrated to enhance energy efficienciesobjective function in harmony search algorithm to develop a balance between dissipation of network energy and controlling of path length. Hence, it becomescompulsoryinselectinginitialenergynodes in a random manner from a specific range as path energy utilization can be small value in selecting a route which takes into consideration of the residual energy. A path is selected to develop balancing among stabilization energy of network and reduced remaining energy.

(TERP) Trust and energy aware routing protocol which is intended to explain before mentioned restrictions is put forth by Ahmed et al. [22]. TERP design and development is centered on energy efficiency and trustworthiness keeping resource- restricted characteristic of WSNs in mind. Duringtrust assessment phase TERP is capable of isolating after dynamically detecting misbehaving nodes. Energy awareness characteristics are infused inroute setup phase helping in load balancing nodes that are validated and trusted. Depending on hop counts, trust and energy TERP uses function of composite routing in which decisions are made. TERP that are joined with an enhanced route maintenance techniques which are intelligently assessed link status that depends on controlled congestion level leading to permanent linkdisruptions and differentiating transient response.

Distribution scheme with inter cluster multiple key for WSNs was introduced by Mehmood et al. [23]. From someof probabilitydependentsecurityand structural schemes cryptography techniques are explained. Utilising pre-distributive key allotment prior to public private key generation and cluster key creation forCH increasing security level of network to a larger extent. Moreover It implement method to include node's ID to production of CH‘s public key. Withmany public keys as explained in this techniquesthus making it more complicated for attackers in decrypting keys, disturbing or attacking whole network systems and hijacking CH. Verification of authenticity of non-malicious and cluster member node is executed in security system in two-phases utilizing CH.

Trust routing and security methods depending on active identification and its characteristics are highly successful scalability, securityandrouting probability that is proposed by Liu et al. [24]. Active-trust techniques can within no time detects nodal trust avoiding nodes that is suspicious to suddenlyachieveapproximately100%successfulprobability in routing.Fordevelopingmanydetecting routesactive-trust methods extensively make use of residual energy. Successful routing probability is enhanced using this scheme upto more than 3 times, and in some cases up to 10 times of previous values.

To –exploreinadequate secure connectivity issues related to its implication on network lifetime, queue size, path length, and energy dissipation Yildiz et al. have provided a solution in linear programming infrastructure [25]. Focus of our work while researching issues of not having a fully connected secure network as its lifetime is a crucialperformance metric in WSNs.We use log–normal– shadowing propagation model for getting precise energyexpenditure vlaues inWSNs,since compared to outcome received under ideal conditions realistic assumptions on radio propagation models have dramatic effects‖ on lifetime.

For –risinglevel of energy consumption Deepa and Latha have put forth a cluster-dependent hybrid hierarchical secure routing protocol [26]. By addinga coordinator node and there by evaluatingefficiency in transfer of packet that relies on packet priority this algorithm explains an improved concept. Capability to transmit packet from source to destination without losing packet to anysuspiciously maliciousnodeandun-capablenodeactivity,packet could be transmitted quickly at destination. By producing a fixed immovable or virtual base station having direct connection to shortest path,coordinator node and its head forming the path, validating packet priority and sending packet‖ to destination end.

For routing protocol –improvingsecurity by trust-based approach Selvakumar et. al. have suggested an intelligent energy aware secured algorithm schemes [27]. To find out minimum distance path amongst sender node and destination node, fuzzyC-means combined with modified minimumspanning tree concept are implemented herethereby selecting an optimal and secured routing path. With the help of CH rotation and modified minimum spanning tree idea providing optimal behaviour such forward control mechanism-based clustering approach generates minimum routes for communication‖ in this systems.

pplying access control and authentication protocol,—Razaque and Rizvi have explained secure data aggregation in [28]. Attacks that are Difficult to be detected by trusted manner this technique is used to identify sinkhole and Sybil that are severe in nature. Secure data fragmentation (SDF) and node joining authorisation (NJA) are two novel algorithm of SDAACA protocol. With fragmenting it into small pieces SDF algorithm conceals information from adversary. To improve QoS parameters NJA algorithm handles authorization procedure. By decreasing communication overhead and providing guarantee to communication validation process an access control methods supports authentication, freshness, accuracy and energy‖ efficiency.

SIGNIFICANCE AND SCOPE

WSN becomes a complicated and challenging taskin giving secure routing, hence large number of research has been showcased. Yet, there remains inadequate information for research and study in routing protocol for WSNs. The contributions: In minimizing control overhead without network behaviour being compromised, protocol of realisable and security aware routing (RSAR) has to be proposed. Conditional tug of war optimisation (CTWO) algorithm is used for processing of trust degree in every sensor nodes proposed RSAR protocol. Later, for optimising consumption of energy apply cluster dependent data aggregation. For providing secure system of trust-based by not regulating energy network lifetime and overhead state-of-the-artis animportantaspectthatisputforth RSAR protocol. Here, we study the importance of energy efficient aggregation methods for secured routing protocols in WSN. Also, we present the review of existing models for efficient aggregation methods of secured routing protocols in WSN.

CONCLUSION

Since main source of energy is limited battery power WSNs, it is highly recommended that WSN, so as to prolonglifespantomaximum possibleprotocolsmust perform in an efficient method. Energy is highly influenced if both multipath routing and security mechanism clubbed together. Therefore, developing robust and lightweight protocols of security very challenging issue. Because of many security and complex solutions, it becomes impossible to develop and design a standalone solution which can attain all aims of security measure. Security measures should be chosen carefully rather, depending on uses, for maintaining an equilibrium amongst security leveland optimal use of resources that are accessible.

REFERENCES

1. C. D. Scott and R. E. Smalley (2013),—Diagnostic Ultrasound: M. Razfar et al.,—Wireless network design and analysis for real time control of launch vehicles, —IEEE International Conference on Wireless for Space and Extreme Environments, Baltimore, MD, 2013, pp. 1 - 2. DOI: 10.1109/WiSEE.2013.6737574.

2. Yu, W. Yuanping, Z. Liang, H. Yuan and Z. Aijuan (2015), —Relay Node Deployment for Wireless Sensor Networks Based on PSO,—2015 IEEE International Conference onComputer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, 2015, pp. 2393 -2398. DOI:10.1109/CIT/IUCC/DASC/PICOM. 2015.353.

3. L. Han (2012), —A Multiple - Hop Energy Efficient Clustered Algorithm for Heterogeneous WSN, —2012 Fourth International Conference on Multimedia Information Networking and Security, Nanjing, pp. 183 - 186. DOI: 10.1109/MINES.2012.36.

4. P. Briff, A. Lutenberg, L. Rey Vega, F. Vargas and M. Patwary (2015),—Generalised trade - off model for energy efficient WSN synchronization —, IEEE Electronics Letter, Vol. 51, No. 3 pp. 291-292.

5. G. Han, J. Jiang, M. Guizani, and J. J. P. C. Rodrigues (2016), —Green routing protocols for wireless multimedia sensor networksǁ, IEEE Wireless Communication, Vol. 23, No. 6, pp. 140-146.

6. T. Hayes and F. H. Ali (2016), —Location aware sensor routing protocol for mobile wireless sensor networks, —IET Wireless Sensor Systemǁ, Vol. 6, No. 2, pp. 49-57.

7. J. Yan, M. Zhou, and Z. Ding (2016),—Recent advances in energy - efficient routing protocols for wireless sensor networks: A reviewǁ, IEEE Access, Vol. 4,pp. 5673-5686, 2016.

8. Wang, Ning, Yuan Zhou, and Wei Xiang (2016), —An energy efficient clustering protocol for lifetime maximization in wireless sensor networks.ǁ In 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1 - 6. IEEE.

9. Muhammad Arshad, NasrllahArmi, NidalKamel, N.M. Saad (2011), —Mobile data collector based routing protocol for wireless sensor networks, —Scientific Research and Essays 6(29) pp. 6162 – 6175.

10. Madhumathy.P, Sivakumar (2014),—Enabling Energy Efficient Sensory Data Collection Using Multiple Mobile Sinkǁ, IEEE magazine, Vol. 11, Issue 10.

11. W. ZHANG, G. CAO, and T. L. A. Porta(2003), —Data Dissemination with Ring - Based Index for Sensor Networks,—IEEE international conference on Network Protocol, pp. 305-314.

12. LON G Cheng, YIMIN Chen, CAN FENGChen, JIAN Ma (2009), —Query - based data collection in wireless sensor networks with mobile sinksǁ, International Conference on Wireless Communications and Mobile Computing, pp. 11S7 – 1162.

13. XIE Dongliang, WU Xiaojie, LI Dan, SUN Jia

(2014), —Multiple Mobile Sinks Data Dissemination Mechanism for Large Scale Wireless Sensor Network‖, IEEE China Communications, Vol. 11, Issue 13.

14. ShanthiVemulapalli and Kemal Akkaya (2010), —Mobility - based Self Route Recovery from Multiple Node Failures in Mobile Sensor Networks‖, IEEE International Workshop on Wireless Local Networks.

15. Wang Liu, Kejie Lu (2012), Senior Member, IEEE, Jianping Wang, Liusheng Huang, and Dapeng Oliver Wu, —On the Throughput Capacity of Wireless Sensor Networks with Mobile Relays‖, IEEE Transactions on Vehicular Technology, Vol. 61, No. 4.

16. P.K. Liao, M.K. Chang and C.C. Kuo(2009),—A statistical approach to contour line estimation in wireless sensor networks with practical considerations, —IEEE Transaction on Vehicular Technology, vol. 58, no. 7, pp. 3579–3595.

17. Jamshidi and M. Nasiri – Kenari (2008),—Performance analysis of transmitter side cooperation receiver - side - relaying schemes for heterogeneous sensor networks,‖ IEEE Transaction on Vehicular Technology, vol. 57, no. 3, pp. 1548 – 1563.

18. U. Lee, E. Magistretti, M. Gerla, P. Bellavista, and A. Corradi (2009),—Dissemination and harvesting of urban data using vehicular sensing platforms, —IEEE Transaction on Vehicular Technology, vol. 58, no. 2, pp. 882 – 901.

19. K. Akkaya, M. Younis, M. Bangad(2005). —Sink repositioning for enhanced performance in ireless sensor networks,—Elsevier Computer Networks, vol. 49, no. 4,pp. 512-534.

20. Jin Wang, Yue Yin, Jianwei Zhang, Sungyoung Lee and R. Simon Sherratt (2013), —Mobility based Energy Efficient and Multi - Sink Algorithms for Consumer Home Networks‖, IEEE access, Vol. 59, Issue 1.

21. KhadijeRahimkhani, FatemehForouzesh (2017), —Improved Routing in Wireless Sensor Networks Using Harmony Search Algorithm‖, Journal of Wireless Sensor Network, 9, pp. 333-353, Scientific Research Publishing.

22. Ahmed, A., Abu Bakar, K., Channa, M., et. al. (2015), —A trust aware routing protocol for energy constrained wireless sensor network‖, Telecommun. Syst., 61, (1), pp.123–140.

23. Mehmood, A., Umar, M., Song, H. (2017),—ICMDS: secure inter - cluster multiplekey distribution scheme for wireless sensor networks‖, Ad Hoc Netw., 55, pp. 97–106.

24. Liu, Y., Dong, M., Ota, K., et. al. (2016).—Activetrust: secure and trustable routing inwireless sensor networks‖, IEEE Trans. Inf. Forensics Sec., 11, (9), pp. 2013–2027.

25. Yildiz, H., Ciftler, B., Tavli, B., et. al. (2018),—The impact of incomplete secure connectivity on the lifetime of wireless sensor networks‖, IEEE Syst. J., 12, (1), pp. 1042–1046.

26. Deepa, C., Latha, B. (2017). —HHSRP: acluster based hybrid hierarchical secure routing protocol for wireless sensor networks‖, Cluster Comput., 22, pp. 1–17.

27. Selvakumar, K., Sairamesh, L., Kannan, A. (2017), —An intelligent energy aware secured algorithm for routing in wireless sensor networks‖, Wirel. Pers. Commun., 6, (3), pp. 4781–4798.

28. Razaque, A., Rizvi, S. (2017), —Secure data aggregation using access control and authentication for wireless sensor networks‖, Comput. Secur., 70, pp. 532–545.

Corresponding Author

Kulkarni-Shinde Bharat Pralhad*

Ph.D. Student, SunRise University, Alwar

E-Mail –