Journal of Advances in Science and Technology
Vol. 16, Issue No. 1, March-2019, ISSN 2230-9659

A Detailed Review on Security and Energy-Efficiency of Routing Protocols in Wireless Sensor Networks

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

[1] Ph.D. Student, Sunrise University, Alwar, Rajasthan

[2] Professor, Ph.D. Guide, Sunrise University, Alwar, Rajasthan

[3] Principal, Shri Chhatrapati Shivajiraje College of Engineering, Pune - 412205

Abstract – The Wireless Sensor Network (WSN) has got much importance these days. With the tracking and monitoring activities become essential, the deployment of sensor networks through wireless medium have also increased. Although sensors are unavoidable in many fields, they got many issues pertaining to energy, routing, security, coverage, delay, architecture etc.; There are many on- going researches in the field of wireless sensor networks. The enhancement of lifetime of sensors has become an important area of research. The fact that a sensor being a micro electronic device, equipped with limited power source. The power source supplies energy needed by the device for processing. If the nodes are deployed far apart, recharging and replacing are tedious process. Apart from hardware issues, the utilization of energy also plays a vital role. The energy go waste in many cases that includes, idle listening, retransmitting, overhearing, over-emitting. To accumulated information in Wireless Sensor Networks (WSNs) large number of inexpensive, lightweight sensors can be arbitrarily spread in harsh and open environment. Hostile conditions as well as low battery life span of battery-operated sensors, need research and development of reliable, secure and energy-efficient sensor network protocols. Out of broad range of network protocols that is routing, is most crucial in terms of utilization of energy, as information interchange consumes 70% of entire energy in wireless sensor networks (WSNs). Due to which, so as to conserve energy and improve network's lifetime routing systems with energy efficiency must be developed. But, application-specific nature, lack of a global solution scheme and resource-limited sensors of WSNs proposes a critical challenges for implementing routing of information. Moreover, privacy and security is another critical issues in WSNs, as sensors has to be typically placed in least secured environment and prone to security attacks and phishing. To cater security objectives various currently existing routing protocols have many security measures present in systems. Different energy efficient and secure routing protocols in wireless sensor networks is showcased by us in brief review, focussing on underlying operations and principles.

Key Words – Routing, WSN, Energy Efficiency and Security

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

1. INTRODUCTION

WSN acronymic for Wireless sensor network has an important role in domestic use finds application in military department. These systems are seldom uses utmost sensistive and personalise information such as report acquired from sensors placed on various parts of body, for keeping track of medical condition of critical petients, where entire types of decision and prescription selected depending on information provided by sensors. Various methods and algorithms came into existence, out of which trust-based algorithms are more beneficial compared to conventional methodologies. Such kind of techniques gives ultimate availability, integrity with security, validation of information at all nodes in systems. During installation of trust-based techniques resulting in difficulties such as data congestion into system, because of Information overflow that is very complicated issues. Figure1shows the architecture of WSN.

Overall lifespan of network is severely brought spiralling down which directly affects process of data aggregation, as a cascading influence. In this research we suggest a protocol of secure aware routing (RSAR) that is safe and realisable. This technique is used to surpass existing problems. It initiates by starting with trust factor measurement of every sensor node in systems. By applying

conditional tug of war optimisation algorithm, output values are computed by method of optimal trust inference. Information aggregation assists in decreasing instantaneous flow of date in saperate node to multi-hop and segregates required information saperately, later sending collected data at receiving end. By passing multiple and fault data from accumulated data and in turnimproves WSN lifespan by saving its battery, Efficiency of Energy in this suggested task is received. By evaluating trust factors this method help in finding out data assaults and mitigate.

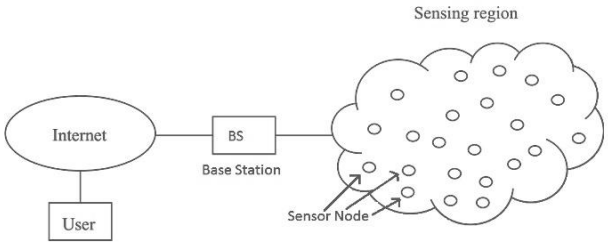

Figure1: Architecture of WSN

Requirement for more effective security methods is ever increasing in demand because of non-stop growth of WSN technology. From initiation in designing of system security concerns of sensor network in systems should be addressed properly, as they communicate with sensitive information and naturally processes in hostile unattended atmosphere. An in depth knowledge of capabilities and restriction of every underlying technology is needed for security protocol development.

For overcoming condition such as attacks and nodes malicious nature WSN should be designed in an efficient manner, as in various ways malicious node interrupts with distortion of data transmission like Doppler effect and multi-path. Because transmitting node sends information along a separate path in case of event such as crucial junction node becoming malicious resulting in receiving both data interference at destination possibly generates an error or repeated messages such as disturbance. Conditions such as message distortion, impersonating, interference, message replay eaves dropping and leakage of top-secret information can be created by an attack.

Hence, it becomes compulsory to have knowledge about trust affected constraints to develop beneficial security mechanisms while accepting and implementing concepts from recent security methodologies. Depending on data aggregation model and interference of optimal trust issues like these are overpowered by an RSAR protocol conept. For computing level of trust degree in every sensor nodeCTWO based trust inference model is applied. For grouping nodes with base of good degree of trust, cluster-dependent data aggregation which is energy efficient is implemented, which result in enhancement of information forwarding by decreasing in attack contribution for next forwarding nodes in a systems.

2. 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 guideline to 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 in WSN 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 on split tree techniques shortest transmission path 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 QBDC conspire is presented In [12]. Even with 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 throughput

is 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 assortment is improved 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 parameters in consumer network, depending on these EMCA and MECA algorithms are put forth in [20].

Khadije and Fatemeh et. al. [21] proposed an improved Routing in Wireless Sensor Networks using Harmony Search Algorithm. This paper is concentrated to enhance energy efficiencies objective function in harmony search algorithm to develop a balance between dissipation of network energy and controlling of path length. Hence, it becomes compulsory in selecting initial energy nodes 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. During trust assessment phase TERP is capable of isolating after dynamically detecting misbehaving nodes. Energy awareness characteristics are infused in route 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 link disruptions and differentiating transient response.

Distribution scheme with inter cluster multiple key for WSNs was introduced by Mehmood et al. [23]. From some of probability dependent security and structural schemes cryptography techniques are explained. Utilising pre-distributive key allotment prior to public private key generation and cluster key creation for CH 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. With many public keys as explained in this techniques thus 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, security and routing 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 suddenly achieve approximately 100% successful probability in routing. For developing many detecting routes active-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 "explore inadequate 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 crucial performance metric in WSNs.We use log–normal–shadowing propagation model for getting precise energy expenditure vlaues in WSNs, since compared to outcome received under ideal conditions realistic assumptions on radio propagation models have dramatic effects" on lifetime.

For "rising level of energy consumption Deepa and Latha have put forth a cluster-dependent hybrid hierarchical secure routing protocol [26]. By adding a coordinator node and there by evaluating efficiency 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 any suspiciously malicious node and un-capable node activity, 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 "improving security 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, fuzzy C-means combined with modified minimum spanning tree concept are implemented here thereby 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.

Applying 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.

3. SIGNIFICANCE AND SCOPE

WSN becomes a complicated and challenging task in 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-art is an important aspect that is put forth 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.

4. CONCLUSION

Since main source of energy is limited battery power WSNs, it is highly recommended that WSN, so as to prolong lifespan to maximum possible protocols must 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 level and 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 on Computer 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 networks", 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 System", 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 review", 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." 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 Sink", 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 FENG Chen, JIAN Ma (2009), "Query - based data collection in wireless sensor networks with mobile sinks", 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. Shanthi Vemulapalli 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 wireless 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. Khadije Rahimkhani, Fatemeh Forouzesh (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: a cluster 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, Rajasthan