International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Research Trends in Secure Routing Protocols and Communication System in WSNs

Somu Parande, Jayashree D. Mallapur

Abstract: ***At present, Wireless Sensor Networks (WSNs) is fastest growing technology which extensively adopting for various application services including; weather monitoring, traffic prediction, surveillance, research and academic fields etc. As the sensor nodes are randomly deployed in wireless environment, security metrics becomes most promising challenge where communication wirelesses networks facing today. In WSNs, sensor nodes acquires various security concern i.e. vulnerabilities, threats and malicious attacks. Due to the limited resource constraints like bandwidth demand, limited memory, computational cost and minimum energy consumption of sensor nodes makes the network security protocols unachievable. In this context, this comprehensive study provides extensive review of WSNs, various challenges mainly related to security attacks and their solution strategies to strengthen the network performance. The significant contribution of this survey study is to provide the comprehensive report on standard secure routing schemes introduced in the literature and pertaining them to secure and non-secure routing protocols for strengthening the WSNs lifetime. Furthermore, the study considers the most frequently used security protocols published between 2010 to 2019, and investigates the major issues towards the security provisions in WSN, which may help for designing a futuristic routing protocol for any WSNs.***

Keywords: Cryptography Algorithms; LEACH; Security Attack; Secure Routing Protocol; Wireless Sensor Network..

I. INTRODUCTION

With the fastest growth of computer networks and telecommunication systems, wireless sensor network (WSN) technology emerge as active and dynamic research area. A typical WSN incorporated with thousands of sensor devices that have inbuilt characteristics for sensing, processing and communication over the wireless channels. However, the major limitations of these networks include dynamic topology, large scale deployment, node mobility, storage energy and constrained, etc. These all resource metrics may directly or indirectly effects on network security system [1]. Though WSN has multiple features and limitations that need to be taken into consideration. For example; network density, where multiple sensor nodes communicating simultaneously, medium access control and network scalability is the major challenge. Another significant limitation is size of the sensor nodes, where each node contains restricted amount of bandwidth, computation and communication capability. These limitations cause several challenges in the design and deployment of wireless networks at different layers of network protocol stack [2].

However, in WSNs secure and efficient routing is the essential factor to perform data transmission tasks. An efficient routing is the process of selecting appropriate route to forward the data packets from source to destination. The entire process is carries out at network layer where nodes are responsible to collect the data from the participant nodes and forwards the data packets to sink node and turn forwards the processed data to the end user [3]. However, WSNs employs various cryptography based routing protocols to ensure the secure communication between the nodes or networks. Due to the dynamic characteristic of WSNs, these networks are more vulnerable for various malicious attacks such as; Black hole attacks, eaves-dropping attacks, Denial of Service (DoS) attacks and Distributed DoS attacks, etc [4]. In WSNs, intruder node may cause interferences leading to data communication or transmission failure between the sensor nodes. Robust and efficient routing protocols can be utilized to mitigate this problem and prevent the network from malicious attacks.

The verities of routing protocols have been investigated by different researchers and utilized to strengthen the communication mechanism over the WSN environment. The significant role of a reliable routing protocol is to establish a communication link and packet transmission over the network. The communication process among sensor nodes is administrated by routing protocols; therefore the overall performance of the any wireless network mainly depends upon adoptive routing strategy. Multiple numbers of energy efficient and secure routing protocols have been designed and implemented for various application services in order to enhance the communication performance of the WSNs [5]. In this context, the present comprehensive survey study classifies the routing protocols into three different categories viz; i) Mode of function, ii) Based on node performance, and ii) Network Structure (Shown in figure-1).

A. Motivation

The present survey study done in the state of art of secure wireless communication network,

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author
Somu Parande*, Assistant Professor, Department of Electronics & Communication, Basaveshwar Engineering College, Bagalkot, Karnataka, India, Email somuparande63@gmail.com
Jayashree D. Mallapur**, Professor, Department of Electronics & Communication, Basaveshwar Engineering College, Bagalkot, Karnataka, India

and can notice that more attention has not given yet for multiple applications to fulfill the all requirement in a single set of network model.

The most recent routing protocols ensure data confidentiality and secure routing for specific networks and resolves particular query. Therefore, the survey study suggests that the designed WSN should fulfill the end user requirements with the ability to balance the tradeoff between confidentiality, routing, communication, and energy efficiency. So, the comprehensive survey study mainly focused on prior routing protocols which provide secure communication.

The organization of survey study is arranged as; section-II provides the literature review of existing methods. Section-IV illustrates the new research trends in secure routing protocols, followed by research gap in Section-V. Finally, section-VI defines the conclusion of the survey study.

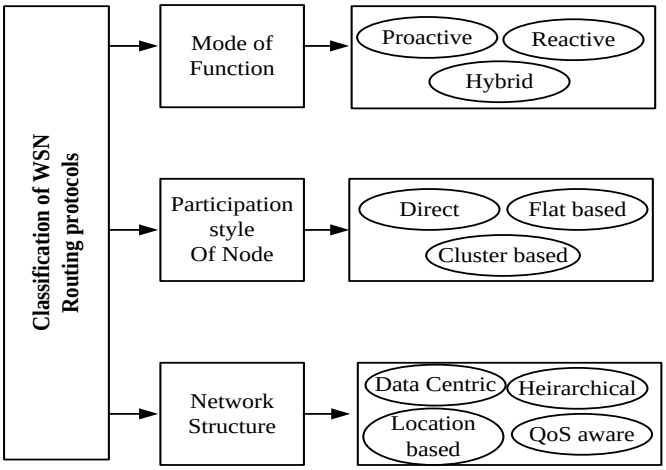

Fig. 1.Classification of Routing Protocols

The above figure represents the generalized classification of WSN routing protocols. The table-1 highlights the most prominently used routing protocols and is considered in the frequent research studies to resolve the security problems [6]. According to the literature review, the most commonly utilized WSN routing protocols are Data centric, Location based and Hierarchical routing protocols. The data centric routing protocols performs based on query processing to degrade the transmission failure problems. Location based routing protocols performs data transmission to the sink node using the position of node information. Hierarchical routing protocols works on clustering based policies and aim is to reduce the energy consumption rate during data aggregation and data transmission process.

Till date, there are various research studies has been concentrated on WSN security problems, in which gained more attaintion to enhance the WSN security with minimum energy consumption. The most prominent survey papers [7], [8] focused on security problems. However, with respect to security concerns none of the research study provided efficient solution till now, this survey study conclude that it was quite challenging task to understand the effectiveness of the prior techniques. The study strongly believe that security features can be incorporated with multiple parameters including delay, bandwidth, energy and etc, and it is not necessary to include cryptography schemes only. The closer look at the research trends shown in figure 2 which illustrates that transaction papers published over IEEE Xplore is very less. Figure 2 (a), (b) and (c) are quite less focused cryptographic techniques and can notice that more number of journals certainly do exists. Additionally, figure 2 (d) provided information on trust and reputation based security techniques which have limited research studies to till date. It shows only six research papers are published in IEEE Xplore worked on trust and reputation based technique to provide secure communication over the WSN environment. The similar research efforts can also be seen in other standard publishers including Springer, Inderscience, Elsevier, etc.

Table 1. Comparisons of different routing protocols based on performance metrics

Class of Routing protocol	Example	Energy usage	Localization	Mobility	Security requirement
Negotiation based	SPIN [19]	Limited	No	Yes	Restricted
Hierarchical	LEACH [10]	Maximum	Yes	Fixed	High
Hierarchical	TEEN [11]	Maximum	Yes	Fixed	High
Grid-based	PANEL [12]	Limited	Yes	Yes	Restricted
Chain-based	PEGASIS [13]	Maximum	Yes	Fixed	High
Location-based	GPSR [17]	Limited	No	Limited	Restricted
Location-based	GEAR [18]	Limited	No	Limited	Restricted
Event based	QoSRP [21]	Limited	Yes	Yes	More

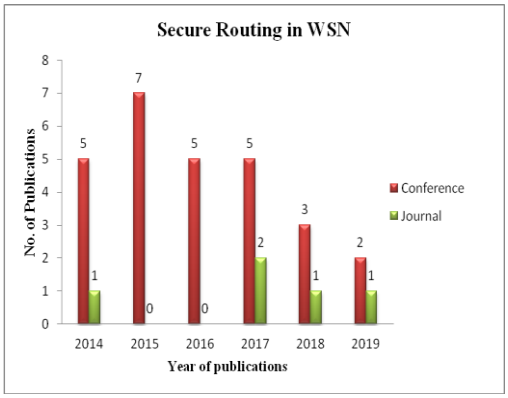

Fig.2 (a) Research work on Secure Routing in WSN

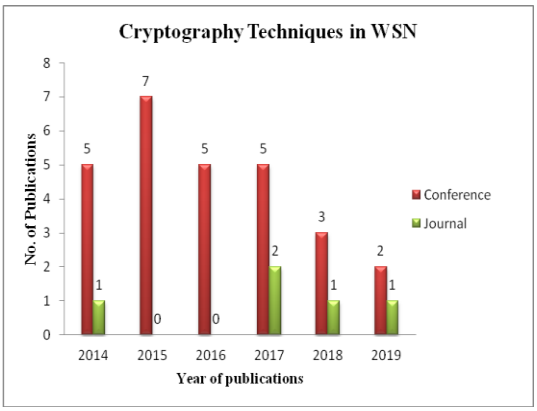

Fig.2 (b) Research work on Cryptography Techniques in WSN

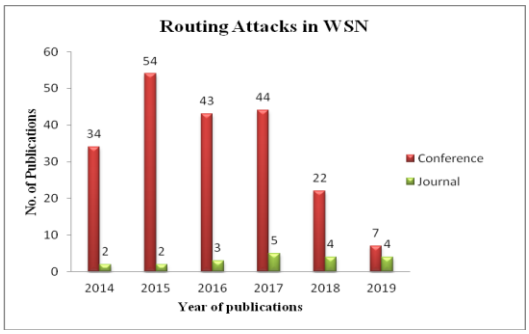

Fig. 2 (c) Research work on Routing attacks in WSN

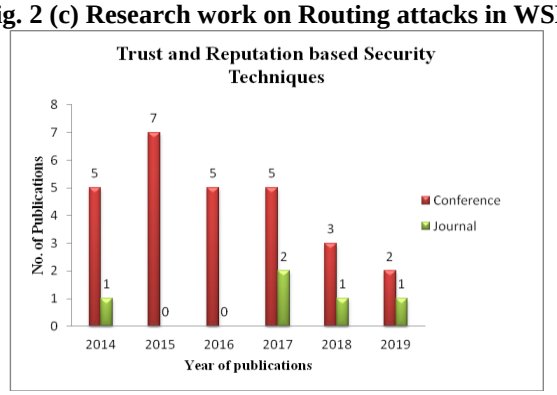

Fig.2 (d) Research work on Trust and Reputation based security Techniques

II. RELATED WORK

There are various approaches presented by different authors pertaining to both secure and non-secure routing protocols over WSNs. This section discusses the current and most frequently used techniques of research published between 2010-2018.

Initially, there is various literature studies focused on reviewing search problems on secure routing in WSNs. Subsequently, existing studies considered several issues like as energy efficiency [9], location-based [10], Network topology [11] [12], network scalability and maintainability [13], effective data transmission [14], multipath routing and secure multi-path routing [15] [16] and security [17] etc... All those investigational studies provide a detailed study of different routing schemes. However, this section is mainly focusing on a comprehensive survey study of secure routing protocols in WSNs.

Ishmanov and Zikria [18] proposed a trust-based mechanism with secure routing strategy for WSNs and explored the current research study and identify the open research challenges by surveying proposed mechanisms. Later, they classified the prior routing protocols based on the type of routing attacks and presented comprehensive research on a trust-based mechanism to secure the routing in WSNs.

Kaur et al. [19], presented a trust-based secure routing mechanism that establishes a trustworthy secure routing between each sensor nodes to the destination node. The significance of the proposed routing protocol is to obtain information securely and protect the performance of the network from degradation and other resources. From this approach can protect information exchange, secure data delivery as well as update the rout by isolation of malicious nodes.

Rahayu et al. [20], introduced a combinational approach of secure routing protocol and secure data aggregation protocol i.e., the study proposed a LEACH-based secure routing protocol (SLEACH) so as to optimize the security level of any data-aggregation protocol. The principal motive of the proposed study is to show the significance of considering SLEACH and secure data-aggregation together in designing a routing protocol for any WSNs to attain energy aware secure routing protocol.

The most recent, Fouad et al. [21], proposed an adaptive routing mechanism for WSNs, which is responsible for enhancing the WSNs performance using the dynamic multi-routing scheme. The aim was to find the shortest path among each node to the sink node. Due to this, it can consume less power and maintain the power consumption throughout the network by transmitting the limited data packets for every node. Additionally, it can reduce the data redundancy at the transmission process. In Kumar et al. [22], have designed a significant security routing protocol for heterogeneous WSNs. The proposed protocol can identify the trusted adjacent sensor nodes in heterogeneous WSNs and discover a secure routing for secure data transmission.

The proposed protocol adopted an ECC public key algorithmic approach to offer higher security for data delivery. Authors have shown that from the proposed routing protocol can reduce the computational complexity as well as improve the data combination efficiently. Additionally, the proposed protocol has drastically mitigated the storage requirement and energy usage at every sensor node within the network area through efficient key-management approach as compared with other existing approaches.

In every WSN, the most critical challenge is the energy consumption and prolongs the network lifetime, since that sensors can be energized by batteries in most cases. Therefore, by considering this issue, Lin and Donghui [23] proposed energy balanced routing protocol for WSNs. They adopted the fuzzy logic and k-means clustering approach to prolong the network lifetime. Also, they designed a genetic algorithm to obtain the fuzzy rule for various sizes of sensor networks.

Another energy-efficient routing protocol (EE-RP) has been introduced by Khan et al. [24] i.e., multi-stage packet transmission scheme and proposed a CHs selection algorithm. The proposed algorithm utilized for efficient selection of CHs. Finally, the performance metrics and EE-RP are measured by comparing the results with existing protocols (i.e., LEACH and MoD-LEACH).

Sung et al. [25], proposed an energy efficient routing protocol, which can offer the quality of services in terms of reliability and delay. The agenda was to minimize the routing control information's and hence can securely operate from energy-efficient perspective. From the result analysis, they proved that can broadcast the messages and sensor node can easily transmit the data to sink node by establishing of shortest route path as well as converse the energy.

In the research study of Li and Chuang [26], proposed a location-based energy efficient multipath routing protocol. By applying this mechanism can divide the entire network structure into several clusters and simultaneously sends the data packets through the clusters without interrupting to others. The main objective was to attain free-interference data transmissions. The proposed scheme handles a load of every cluster as per to the energy capacity of their nodes. The protocol doesn't discover a fixed routing path in advance, and therefore, it upholds high performance even if the topological structure change instantly.

Another most important factor to be tackled in any WSN is the network-lifetime. By considering this point, in [27], Saleem et al. introduced an empirical study on self-configurable autonomous, secure routing protocols. The primary intention was to minimize packet loss, delay, and energy consumption on WSNs. In this research, authors presented an architectural design along with experimental results of the proposed routing protocol. Finally, from the experimental study, they concluded that the proposed protocol provides high performance and can be implemented in real time WSN applications, e.g., environmental monitoring and surveillance systems.

Trust-based secure routing scheme is proposed by Qin et al. [28], to analyze the behavior of the sensor node, along with data transmission and energy consumption of the sensor node. Here proposed system evaluated the frequency of sensor node and discovered the optimal path from the source node to the sink node. Simultaneously, trust-degree and QoS parameters are integrated as routing measurements, which represents the optimized routing scheme by applying the semiring approach. Finally, from the simulation outcomes, they showed that the proposed routing protocol improves security as well as the effectiveness of WSNs.

An extensive set of data is exchanged over the WSNs; as a result, the challenge is how to improve the network throughput in service-oriented wireless networks. Therefore, Li et al. [29] have introduced service-oriented network architecture for WSNs. The proposed secure routing protocol scheme provides multiple features like i) data delivery with security, ii) application independent, iii) extensibility, and iv) secure load balancing. The system performance metrics were calculated in terms of evaluating packet deliver, end to end delay, and overall throughput.

In another research study, Ganesh and Amutha [30], have introduced a secure routing protocol for WSNs using dynamic clustering approach. In this context, the entire network is partitioned in terms of clusters and selects the appropriate cluster-head based on energy factor, and remaining nodes are connected with particular cluster-head based on SNR values. The network security has been achieved by malicious nodes isolation exploiting sink based routing algorithm. From the proposed mechanism can achieve energy consumption and high packet delivery.

Liu et al. [31], have proposed a secure multi-path routing scheme and formulated a system optimization problem that maximizes the network security as well as network lifetime. Theoretical analysis and experimental results showed that the proposed multi-path routing mechanism outperforms in both security and lifetime under different metrics.

Zhan et al. [32] have designed a robust trust-based routing model for dynamic WSNs. The aim was to secure the multi-hop routing networks against malicious attackers. The main focus was on energy consumption and trustworthiness, which are the essential factors that secure the WSNs in a hostile environment. Also, a Tiny-OS framework is implemented for trust-based routing with minimum overhead.

In Taherian et al. [33] designed a secure and optimized routing protocol for WSNs by introducing swarm optimization algorithm. The primary emphasis was to adopt an AI approach to find a secure and efficient route in WSNs along with capable of aggregating the received information from the network and informing it to the activators.

Xiao et al. [34] proposed an energy optimization problem with secure routing scheme for heterogeneous WSNs. They introduced an improved anti-colony algorithm which determines the low-cost routing from cluster heads to base-station. From the simulation results shows that, can easily find the router attackers also observe the variation in data traffic and energy consumption rate.

Chen et al. [35] have designed a secure routing algorithm (i.e., BCDTV) which defines the easy way of selection of cluster-head and cluster establishment method. From this approach can aggregate and transfer the sensing information all over the network environment. The experimental results showed that the proposed routing protocol effectively prevent the network from malicious attack.

In Ahmed et al. [36] introduced energy and trust-aware secure routing scheme for WSNs i.e., TESRP, which adopted a distributed trust-based approach for establishing and separating malicious nodes. Additionally, they showed that this approach could balance the energy as well as traverse the node via the shortest path. Also can achieve high energy consumption, throughput, and enhancement in network lifetime.

Mariano et al. [37] proposed a secure geographic routing protocol for both Adhoc as well as WSNs. In this paper, they utilized a lightweight localization method which allows for the detection of intrusion and prevents the network form several attacks (e.g., sink hole, black hole attacks). In the end system, précising localization and secures routing is evaluated and experimented in real time WSNs and Ad-Hoc networks.

In the research study of [38], [39] and [40] authors proposed secure cluster based and energy efficient routing protocols which help for appropriate cluster head selection as well as the shortest path for secure data transmission.

The following table.2 briefly discusses about existing approaches to secure routing protocols for any WSNs.

Table. 2 Highlights the existing approaches to secure routing protocols for any WSNs

Authors	Problem Statement	Technique	Outcomes	Advantage
Ishmanov and Zikria [18]	A trust-based mechanism to secure routing for WSNs	Comprehensive Survey study	Articles related to specific attacks.	-N/A-
Kaur et al. [19],	To establish a trustworthy secure routing in WSNs	Trust-based secure routing protocol	Comparisons trust-aware routing protocols with the proposed scheme	secure data delivery and can update the rout
Rahayu et al. [20],	Secure data aggregation with secure routing.	SLEACH, MS-LEACH	Security, energy efficiency	Improve security during the data aggregation process.
Fouad et al. [21]	Shortest routing path and energy optimization	Multi-attribute decision-making approach	Fault tolerance, scalability	Can create a routing path as per user performance, reconfigure the network state.
Kumar et al. [22],	Strong security for heterogeneous WSNs	Elliptic curve Cryptographic algorithm	Memory requirement and energy consumption with respect to secure routing protocols	Can reduce the memory requirement and energy preservation.
Lin and Donghui [23]	Energy consumption	K-Means clustering, Fuzzy logic	Balance the energy consumption	prolong the network lifetime
Khan et al. [24]	Multi-path data transmission	Cluster heads (CHs) selection algorithm	Throughput, energy efficiency	Enhance the overall network lifetime
Sung et al. [25],	To provide an energy efficient QoSs	QoS based routing algorithm,	Reliability, delay, energy consumption	Can reduce the routing control information and discover the shortest route towards the sink node.
Li and Chuang [26],	Location-based energy efficient free-interfering multipath routing system	Experimental analysis	End to end delay, data rate, energy distribution	Well balanced energy consumption, load distribution for sensor nodes.
Saleem et al. [27]	Autonomous, secure routing protocol	Empirical study	Delay ratio, throughput, energy consumption	Can be implemented in real time WSN applications e.g., environmental monitoring and surveillance systems.
Qin et al. [28]	Trust-based secure routing scheme for WSNs	Semiring theory	Data reliability, energy consumption	Improve the network lifetime and reliability of data transmission.
Li et al. [29]	Service-oriented framework model for multipath routing with security	Secure load balancing algorithm	Packet delivery, end to end delay and throughput	Improve the network performance

Ganesh and Amutha [30]	Secure and energy efficient routing protocol	Dynamic clustering approach	Packet delivery, end to end delay	Multi-hop wireless communication, a high transmission rate
Liu et al. [31]	Secure and energy efficient multi-path routing scheme for WSNs	3-phase disjoint multipath routing theory	Transmission rate on total energy and on network lifetime	Improvement of network security for both single and multi-black holes.
Zhan et al. [32]	Trust-based routing model for dynamic WSNs	Experimental analysis	Multi-hop data delivery	Provides trust-aware and energy efficient route
Taherian et al. [33]	Design a secure and optimized routing protocol for WSNs	AI approach (i.e., Swarm optimization algorithm	Data aggregation	Can optimally aggregate the received data from the network.
Zhenghong et al. [34]	Detect anomaly with a secure routing protocol for Heterogeneous WSNs.	Anti-colony algorithm	Low energy consumption,	high data transfer with high detection rate.
Chen et al. [35]	Secure routing algorithm	Node convergence and trust-based routing algorithm	Energy and communication rate	Can detect the malicious nodes.
Ahmed et al. [36]	Energy and trust-aware routing scheme for WSNs	Multi-hop routing strategy	Energy consumption, network lifetime	Improve network performance.
Maiano et al. [37]	Secure location-based routing protocol for WSN and Adhoc networks	Lightweight localization method	Packet loss vs. malicious node	Defense from black-hole, sink-hole, etc.
Long and Choi [38]	Low energy consumption in WSNs	Theoretical analysis	No. packet vs. No. sensors	Improve network performance.
Maitra et al. [39]	Secure routing scheme for secure data transmission	Id-based scheme	Comparative analysis	Secure communication for WSNs

From the literature study, have recognized that various routing protocols talks about various security measurement over the WSN. The proposed comprehensive survey study illustrates brief overview and provides significant contributions towards WSN security system by considering routing performance, methodologies and simulation tools. The following figure-5 shows the statistical analysis of existing research work towards WSN security which mainly considers the some significant performance parameters. The study summarized the various routing protocols and security parameters and respective solution strategies using cryptographic approach. In the last have segregated the most prominent research papers and considered authors contributions with unique methodologies and experimental analysis. From the statistical analysis can figure outs that, most of the existing studies majorly focused on energy conservation factor, while very less research work has been done in the field of reduction of communication and computation cost. The reduction of communication overhead is the significant research topic in the state of art of WSN security. WSN have very less resources and security system introduced additional communication overhead. Hence it is essential to develop a security mechanism to strengthen the network lifetime during communication process.

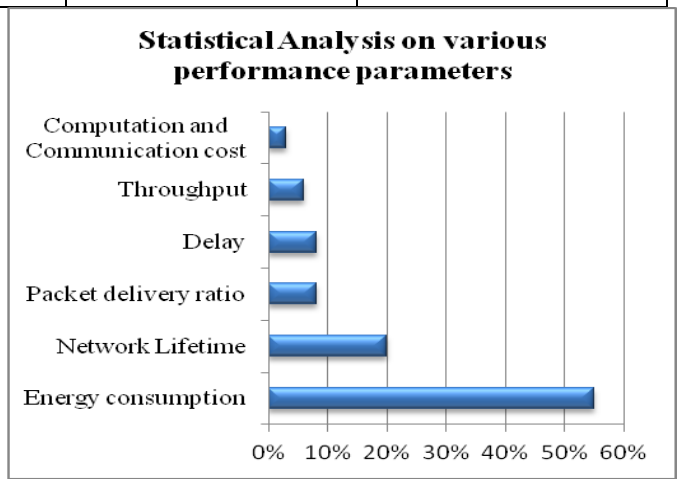

Fig.3. Statistical Analysis of Existing research work with respect to various performance parameters

III. FUTURE TRENDSIN SECURE ROUTING PROTOCOLS

From the extensive research study, can notice that few security-related challenges need to resolve. By pointing out those issues, the rest of this section discusses them as a future study.

A. QoS Assurance and energy efficiency

Nodes energy utilization is the fundamental factor in developing routing protocols for any WSNs to extend the lifetime of conventional WSNs. Nevertheless, adopting such energy efficient routing protocols in multimedia WSNs may result in energy loss due to the redundant or large data transmission on such networks. A suitable solution is proposed in [41] which resolves the energy loss problems and provide QoS oriented routing scheme which optimized the energy as well as QoS assurance among the sensor nodes and the sink node. A secure multi-path routing can be explained in two ways; 1) it can be intended by multi-path exploration while retaining a single-route randomly during the packet transmission process. The aim of random path selection is to distribute the energy between the discovered paths equally. In this routing, the scheme can improve the reliability as well as strengthen the network security. 2) A secure multipath routing can also be attained by discovering multiple paths and employing them for containing distributed message along the discovered routes simultaneously. From this mechanism can minimize the end to end packet delay and detect and prevent from sinkhole attacks. The multipath routing mechanism also provides the QoS assurance needs more research for examining the tradeoff between QoS parameters and energy efficiency.

B. Network dynamics

Most of the conventional WSNs are static. However, advanced technology shows that mobile nodes in WSNs have promising performance. Additionally, the current study on data aggregation exposes that data reporting via implementation and leveraging mobile sink is promising for energy efficient data aggregation than data reporting through multi-hop to static sink node. Thus, the prior study [22] [32] showed that networks which implemented mobile sink contain a high performance over the networks, the sink mobility discovers many challenges that need more consideration for further study. Example: the mobility of sink introduced the sink duplication attack. This may leak confidential information for the public or save it from reaching the authorized node. Thus, security is the main factor to resolve this kind of challenges in both static and dynamic network topologies.

C. Security in multipath routing protocols

For any WSNs, security is becoming an essential factor because of the subjecting of several routing attacks (e.g., sinkhole attacks, warm hole attacks, Sybil attacks, DoS attacks, etc.). Thus, in [42], researches introduced several types of secure routing protocols to prevent the network from these attacks. Nevertheless, new trends and new application in the research technology may require advance secure routing algorithms strengthen the security on WSNs.

IV. RESEARCH GAP

There are various approaches that have been investigated in recent times associated with the security problems of WSN. It must be noted that existing system does offer some excellent security towards data as well as towards communication system in most of the cases; however, there are still some open-ended issues towards the security solution which is an alarming concern if WSN has to be a part of futuristic networking technologies. Following are certain research gap explored after reviewing existing studies:

- *More hypothetical and less practical approach:* Existing approaches towards WSN security problems are constructed on the basis of theoretical hypothesis without considering various problems as follows:
- *Intrinsic problems:* Implementation of security protocols demands the availability of flexible memory as well as storage sectors within a node. Unfortunately, owing to the lesser availability of storage, it is never feasible to implement high-end encryption approaches in WSN. Apart from this, the allocation of resources for executing such security protocols is very vague from the energy modeling concept in WSN. There is no standard practical energy efficient security protocol that has been proven to be resistive against practical threats in WSN.
- *Extrinsic problems:* The selfish/vulnerable nature of node may be caused due to limited resources as well as the consequence of adversary. However, at present, there is no such research work to claim the origination and identifiable limits of a selfish/victim node. Apart from this, the security protocols are never studied with respect to different networking impediments like interference, scattering, fading, etc. that is very much common in any wireless network. It is also feasible for an adversary to mimic such problems in the form of threat which goes undetected to attack in core networks. At present, there is no such practical solution to this problem.
- *Low emphasis on grass-root problems:* Every research work starts its discussion by assuming that there is an existence of some form of a specific adversary in WSN, and then the authors present their solution. However, little, they discuss if the adversary changes its strategies during the process of implementation of security protocol. In case the attacker adopts a dynamic strategy to launch attack than it can easily bypass any firewall system as any firewall system used has only some limited predefined information of threat levels. It is needed to understand that no attacker directly launches their attack in a practical scenario, and they will need to wait to gain some good trust to make its way inside the network. Such entry is gained by assisting the node to forward data and increase its reputation. It will mean that route request and route reply message forwarded by such node should not be relied upon. At present, there is no such report of standard work that emphasized the identification of legitimacy of the incoming request and its intention of future.

V. CONCLUSION

The significant contributions of this survey study, explored the several routing protocols to realize the secure routing for WSNs. Also, the study highlighted some critical characteristics influencing secure routing protocol design, and provides a comparative analysis among different routing protocols in each category. Furthermore, they have addressed some significant performance metrics in routing protocols, which help to solve the several challenges in WSNs.

However, it is noticed that, most of the research studies adopted cryptographic approaches which is much higher than non-cryptographic approaches. There is an advantage of adoption of cryptographic technique for robust authentication, but the implementation nature is recursive and repeatedly performs the encryption operation. Therefore, more amount of memory space is required for this, which is the major pitfall. The adoption of non-cryptographic approaches is carried out mainly using mathematical modelling and probability theory. In the past few years of research studies has found limited implementations in the form of mathematical-modeling. Hence, our future research work has the aim to develop mathematical modelling based security system and whose functionality will permit detection of uncertain nodes and is capable to address the most difficult forms of adversaries in sensor network. Finally, the research gap is carried by considering significant issues towards the security in WSN, which may help for designing a futuristic routing protocol for any WSNs.

REFERENCES

1. S.K. Singh, M. P. Singh, and D. K. Singh, “Routing protocols in wireless sensor networks–A survey”, International Journal of Computer Science & Engineering Survey (IJCSES), Vol.1, no. 2, pp.63-83, 2010
2. I.S. Hammoodi, B. G. Stewart, A. Kocian and S. G. McMeekin, “A comprehensive performance study of OPNET modeler for ZigBee wireless sensor networks”, In 2009 Third International Conference on Next Generation Mobile Applications, Services and Technologies, pp. 357-362, 2009.
3. A.M. El-Semary, M.M. Abdel-Azim, “New trends in secure routing protocols for wireless sensor networks”, Int J Distrib Sens Netw, 16, 2013
4. M.R. Ahmed, X. Huang, and D. Sharma, "A taxonomy of internal attacks in wireless sensor network”, Memory (Kbytes), 128, pp.48, 2012
5. S. Omar, O. E. Ghandour, and A. M. A. E-Haleem, “Multipath Active Based Routing Protocol for Mobile cognitive Radio AdHoc Networks”, Wireless Communications and Mobile Computing, 2017.
6. G. Nandini, J. Anitha, “Performance Chronicles of Multicast Routing Protocol in Wireless Sensor Network”, International Journal of Advanced Computer Science and Applications, vol. 8, no. 9, pp.284-293, 2017
7. H. Singh and D. Singh, “Taxonomy of routing protocols in wireless sensor networks: A survey”, In 2nd International Conference on Contemporary Computing and Informatics (IC3I), pp. 822-830, 2016.
8. E.Hassan, K. Bourgba, and M. Ouzzif, "A survey on flat routing protocols in wireless sensor networks", In International Symposium on Ubiquitous Networking, Springer, pp. 311-324, 2015..
9. El-A. Mohamed, and M. M. A-Azim, “New trends in secure routing protocols for wireless sensor networks”, International Journal of Distributed Sensor Networks 9, no. 5 , 2013
10. M. Khalid, Z. Ullah, N. Ahmad, M. Arshad, B. Jan, Y. Cao, and A. Adnan, “A survey of routing issues and associated protocols in underwater wireless sensor networks”, Journal of Sensors, 2017
11. H. Echoukairi, K. Bourgba, and M. Ouzzif. "A survey on flat routing protocols in wireless sensor networks." In Advances in Ubiquitous Networking, pp. 311-324. Springer, Singapore, 2016.
12. S.P. Singh, and S. C. Sharma, "A survey on cluster-based routing protocols in wireless sensor networks", Procedia computer science 45 (2015): 687-695.
13. J. Kumar, S. Tripathi, and R. K. Tiwari, "A survey on routing protocols for wireless sensor networks using swarm intelligence." International Journal of Internet Technology and Secured Transactions 6, no. 2 (2016): 79-102.
14. H.D.E. Al-Ariki, M.N. S. Swamy, "A survey and analysis of multipath routing protocols in wireless multimedia sensor networks", Wireless Networks 23, no. 6 (2017): 1823-1835.
15. E. Stavrou, A. Pitsillides, "A survey on secure multipath routing protocols in WSNs”, Computer Networks, vol.54, no. 13, pp. 2215-2238, 2010
16. M. Za. Hassan, H.A-Rizzo, and F. A-Turjman. "A survey on multipath routing protocols for QoS assurances in real-time wireless multimedia sensor networks." IEEE Communications Surveys & Tutorials 19, no. 3 (2017): 1424-1456.
17. S. Sathyadevan, S. Prabhakaranl, and K. Bipin. "A Survey of Security Protocols in WSN and Overhead Evaluation”, In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014, pp. 729-738, 2015.
18. F. Ishmanov and Y. B. Zikria, "Trust mechanisms to secure routing in wireless sensor networks: current state of the research and open research issues." Journal of Sensors, 2017
19. J. Kaur, S.S. Gill, and B.S. Dhaliwal, "Secure trust based key management routing framework for wireless sensor networks”, Journal of Engineering, 2016
20. T.M. Rahayu, S-G. Lee, and H-J. Lee, "A secure routing protocol for wireless sensor networks considering secure data aggregation." Sensors 15, no. 7 (2015): 15127-15158.
21. F. E-Hajji, C. Leghris, and K. Douzi, "Adaptive Routing Protocol for Lifetime Maximization in Multi-Constraint Wireless Sensor Networks”, Journal of Communications and Information Networks 3, no. 1 (2018): 67-83.
22. K.A. Kumar, A.V.N Krishna, and K. S. Chatrapati, “New secure routing protocol with elliptic curve cryptography for military heterogeneous wireless sensor networks”, Journal of Information and Optimization Sciences38, no. 2 (2017): 341-365.
23. L. Li, and D. Li. "An Energy-Balanced Routing Protocol for a Wireless Sensor Network." Journal of Sensors, 2018
24. M.K. Khan, M. Shiraz, K. Z. Ghafoor, S. Khan, A. S. Sadiq, and G. Ahmed, "EE-MRP: Energy-efficient multistage routing protocol for wireless sensor networks”, Wireless Communications and Mobile Computing, 2018
25. S-K. Lee, J-G. Koh, and C-R. Jung. "An energy-efficient QoS-aware routing algorithm for wireless multimedia sensor networks." International Journal of Multimedia and Ubiquitous Engineering 9, no. 2 (2014): 245-252.
26. B-Y. Li, and P-J. Chuang "Geographic energy-aware non-interfering multipath routing for multimedia transmission in wireless sensor networks." Information Sciences 249 (2013): 24-37.
27. K. Saleem, N. Fisal and J. Al-Muhtadi, "Empirical Studies of Bio-Inspired Self-Organized Secure Autonomous Routing Protocol," in IEEE Sensors Journal, vol. 14, no. 7, pp. 2232-2239, July 2014.
28. D. Qin, S. Yang, S. Jia, Y. Zhang, J. Ma and Q. Ding, "Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network," in IEEE Access, vol. 5, pp. 9599-9609, 2017.
29. S. Li, S. Zhao, X. Wang, K. Zhang and L. Li, "Adaptive and Secure Load-Balancing Routing Protocol for Service-Oriented Wireless Sensor Networks," in IEEE Systems Journal, vol. 8, no. 3, pp. 858-867, Sept. 2014.
30. S. Ganesh and R. Amutha, "Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms," in Journal of Communications and Networks, vol. 15, no. 4, pp. 422-429, Aug. 2013.
31. A. Liu, Z. Zheng, C. Zhang, Z. Chen and X. Shen, "Secure and Energy-Efficient Disjoint Multipath Routing for WSNs," in IEEE Transactions on Vehicular Technology, vol. 61, no. 7, pp. 3255-3265, Sept. 2012.
32. G. Zhan, W. Shi and J. Deng, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs," in IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, pp. 184-197, March-April 2012.
33. M. Taherian, H. Karimi, A. M. Kashkooli, A. Esfahanimehr, T. Jafta, and M.Jafarabad. "The design of an optimal and secure routing model in wireless sensor networks by using PSO algorithm." Procedia Computer Science 73 (2015): 468-473.
34. X. Zhenghong, C. Zhigang, and H. Changqin. "Secure routing protocol with anomaly detection in heterogeneous wireless sensor networks." International Journal of Mobile Network Design and Innovation 4, no. 3 (2012): 157-163.
35. L. Chen, X. Qi, L. Liu, and G. Zheng. "A security routing protocol based on convergence degree and trust." International Journal of Grid and Utility Computing 8, no. 1 (2017): 38-45.
36. A. Ahmed, K. A. Bakar, M. I. Channa, and A. W. Khan. "A secure routing protocol with trust and energy awareness for wireless sensor network." Mobile Networks and Applications 21, no. 2 (2016): 272-285.

37. M. G-Otero, T. Zahariadis, F. Álvarez, H. C. Leligou, A. P-Hernández, P. Karkazis, and F. J. C-Quirós. "Secure geographic routing in ad hoc and wireless sensor networks." EURASIP Journal on Wireless Communications and Networking 2010 (2010): 10.
38. L.H. Long and E. Choi. "Energy-Efficiency Protocol for Securing the Wireless Sensor Networks." In IFIP International Conference on Network and Parallel Computing, pp. 589-598. Springer, Berlin, Heidelberg, 2012.
39. T. Maitra, Su. Barman, and D. Giri. "Cluster-Based Energy-Efficient Secure Routing in Wireless Sensor Networks." In Information Technology and Applied Mathematics, pp. 23-40. Springer, Singapore, 2019.
40. T. Wang, G. Zhang, X. Yang, and A. Vajdi. "A trusted and energy efficient approach for cluster-based wireless sensor networks." International Journal of Distributed Sensor Networks 12, no. 4 (2016): 3815834.
41. S. S. Jawaligi and G. S. Biradar. "QoS oriented and delay tolerant WSN routing protocol for data gathering in IoT ecosystem." International Journal of Internet Technology and Secured Transactions 8, no. 3 (2018): 469-487.
42. G. Gulhane and N. V. Mahajan, "Securing multipath routing protocol using authentication approach for wireless sensor network." In Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on, pp. 729-733, 2014.

AUTHORS PROFILE

Somu Parande, completed his B.E from Karnataka University, Dharward, India and M.Tech from Mumbai University, India. He is pursuing PhD from VTU, Belagavi, Karanataka, India. His research area is Wireless Sensor Network. He has 18 years of experience in teaching.

Jayashree Mallapur, She has done B.E from Karnataka University, Dharward, India and M.Tech from Gulbarga University, India. She has completed her PhD in 2009 from VTU, Belagavi, Karanataka, India. She has 25 years of experience in teaching.