Review on the Research Evolution on Secure Routing in Wireless Sensor Network

Nasreen Fathima
Assistant Professor,
Department of CSE,
ATME College of Engineering,
Mysore, India

ABSTRACT

Security in routing mechanisms of Wireless Sensor Network (WSN) has become a key aspect of the current research fields where various security issues due to vulnerable attacks in WSN drag the attention of many researchers. This study is intended to investigate some of the existing secure routing techniques for WSN and emphasizes on the existing efficient secure routing techniques. Inferrencing has been done to evaluate the performance efficiency, limitations and the advantages of the different types of existing secure routing techniques. This paper focuses on the state-of-art study of the existing surveys and presents technologies which are emphasized on designing robustness and computationally efficient techniques for secure routing in WSN. This paper also discusses some of the most important and significant findings as well as a brief illustration of research gap for various robust and computational efficient secure routing techniques in the area of WSN, in addition the description of a set of gaps and recommendations will be helpful for future direction of research.

Keywords

Robustness and Computational efficiency, Wireless Sensor Network, Secure Routing Techniques

1. INTRODUCTION

A Wireless Sensor Network (WSN) is a collection of geographically distributed nodes, where nodes are small size battery driven devices deployed over hostile areas. The sensor nodes are connected with each other in Ad-hoc manner, the devices have capability of running various applications and communicating with other nodes within the network and each node transmits its sensing information to a Sink node which collects all the data as a whole from various other nodes after that the total collected measured aggregated data then reach the various applications through a gateway. The sensor nodes can participate in transmitting data to the other nodes within its predefined range [1]. As the wireless sensor network infrastructure is infrastructureless thus some unique topologies of the network enables dynamic adjustment of the individual nodes in a hostile area. WSN is considered as a most prominent and efficient networking technology as so many nodes have CPU power and radio transceiver capacity and can be deployed over a sensing area where most of the conventional networks with fixed infrastructure are insufficient to perform a particular task. As the power source of each node has some limited capacity so the efficient and the throughput of the network is also limited. Various external factors such as weather conditions can affect the performance of the wireless sensor network. Wireless sensor network is already in use of environmental monitoring, habitat monitoring, and defense etc. All the communication within the sensor nodes takes place using the standard routing protocols. Majority of the routing principle in WSN is done either using single-hop or using multi-hop technique. For reference, Fig. 1 shows the classification of existing routing protocols that are also found frequently adopted in research work.

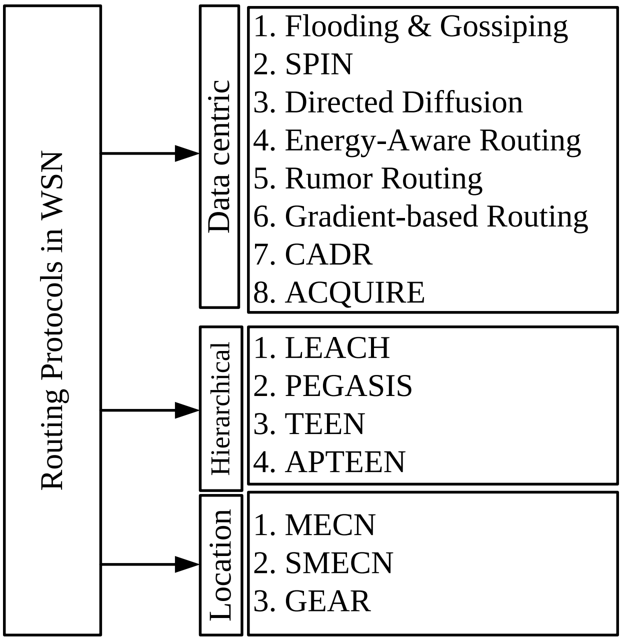

Figure 1 Taxonomy of Routing Protocols in WSN

Some of the unique charecteristics of the routing in WSN are i) complications of undertaking routing principle in static and dynamic scenarios, ii) excess consumption of the energy while performing routing, iii) higher degree of vulnerability of various attack scenarios in the existing routing. However, the prime targets of design and development of routing protocols are to mitigate the energy depletion issues.

The phenomenon of routing is strongly associated with the security systems of the wireless sensor network. As WSN basically comprises of small sensor nodes with limited memory and computational capabilities, hence, it is quite difficult to incorporate complex security or cryptographic based algorithm within the sensor nodes. Even if such work towards including security algorithm is done within the sensor node, it will surely bring forth the tradeoff between the security standards as well as networking (communication) performance of the WSN system.

Therefore, it is highly essential to formulate the security solution considering the routing protocols in WSN. Interestingly, if any algorithm is designed newly, its efficiency is tested using time and space complexity. But, surprisingly, if a security protocol is designed for securing the communication system in WSN, time and space complexity is not enough for performing the effective analysis of the WSN system. It is highly essential that Quality-of-Service (QoS) parameters be considered to testify the effectiveness of the security algorithm with respect to the communication requirements of the WSN. The term communication requirements will mean those variables which directly shows the performance of communication e.g. packet delivery ratio, bandwidth consumption, throughput, energy consumption, latency, bit error rate, etc.

This paper discusses about the security techniques adopted by various routing protocols in WSN. In order to have a better understanding, this paper starts its discussion from the common transmission phenomenon, which is universal in every routing technique in WSN. The paper then discusses about the security vulnerabilities in WSN and finally discusses about the effectiveness of the existing studies. Section 2 discusses about the conventional transmission techniques in WSN followed by discussion on security vulnerabilities in Section 3. Discussion on existing research work is done in Section 4. Various existing studies towards improving the security over routing protocols is discussed in Section 5. Section 6 discusses about the research gap, while Section 7 summarizes the paper.

2. TRANSMISSION MECHANISM IN WSN

The transmission among the sensor nodes in WSN is done in a very typical manner. It is always considered that there are two types of entities in WSN e.g. i) base station and ii) sensor nodes. The base station is meant for collecting the aggregated data and forwards it to the user-based application for data analysis or controlling process for some specific events. The sensor nodes are considered to be two types e.g. cluster head and candidate nodes. Both the types of the nodes can be seen within a cluster of WSN. The candidate nodes are responsible for collecting the raw data from the physical environment and forward the raw data to the cluster head. The clusterhead than perform data processing, removes the possible redundancies and forward the aggregated data either to the base station directly or to the nearest clusterhead of another cluster. It is to be known that candidate node posses lower energy as compared to clusterhead as they (clusterhead) will be required to perform heavy operation of data aggregation. The process of data aggregation consumes maximum energy from the clusterhead. Therefore, it can be seen that clusterhead carries some of the sensitive information, which are of highest interest for the intruder.

In the initial stage of wireless routing the concept of individual nodes to a collective sink node data transmission was suggested as the sensing and the transmission range of each node falls within the location of sink / base station node. It has been observed that in the direct transmission communication technique energy for transmission is directly proportional to the square of the distance between source and Base station/Sink nodes. As a result, the wireless node which resides in farther distance will be considered as a dead node soon. Fig 2 shows the limitations associated with the direct transmission. So large scale data transmission is not appropriate to use in wireless sensor network communication.

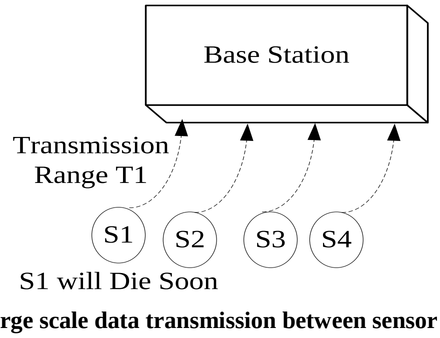

Fig 2: Large scale data transmission between sensor node and Sink/Base Station in WSN.

For mitigating this limitation, a hop to hop communication and data transmission has been introduced where data packets reach the sink node via various other neighbor nodes. The packet transmission/receiving cycle results overhead to the node which stay closer to the sink node, thus it become a dead node soon. Various key management techniques have been adopted to overcome so many security issues [2]. There are various limitations and issues in the area of hop to hop connections which are considered to be more vulnerable to the sensor networks [3]. As a node which stay closer to the base station will deplete more energy as some of its energy will be used in the receiver portion for receive a modulated signal and some of its energy will be wasted for transmitting the data of its own as well as other nodes of the network thus energy consumption will be more in this case.

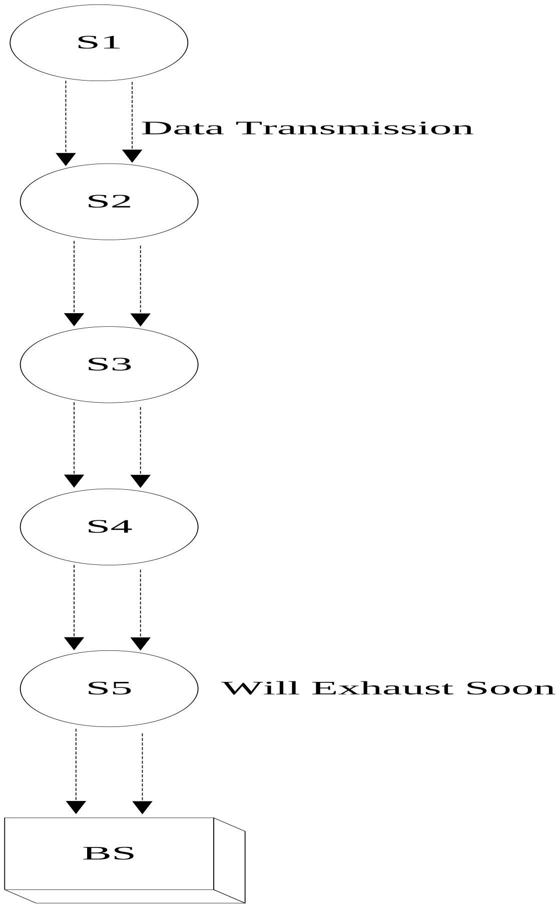

Fig 3: Hop to Hop data transmission between sensor nodes and Sink/Base Station in WSN.

For optimizing these issues, a clustering technique has been proposed where some nodes will form a group or cluster and they will become members of that group [4]. One cluster head will be elected who will collect the information from all the member nodes and process the data for further execution. As the groups are considered here to be static thus the elected leader will be exhausted soon. The exhausted node with no power is termed as a dead node. A concept of dynamic clustering proposed by W. Heinzelman reduces the issues associated with the clustering technique. The concept of low energy adaptive clustering hierarchy (LEACH) has become a bench mark study for the further research direction [5]. There are various routing protocols which are designed for an end to the end data packet transmission with the concept of host-based addressing are considered under topology-based routing protocols. There are many geographic routing algorithms which use position based technique where the destination node is represented by ID. Both the geographic routing algorithm and topology based-routing algorithms are termed as address-centric. Data-centric routing algorithms are very applicable in the area WSNs where queries are generated by the sink to request data packets from the nodes. Single path strategy is also a routing method where one instance of a data packet will be present in the network at a time.

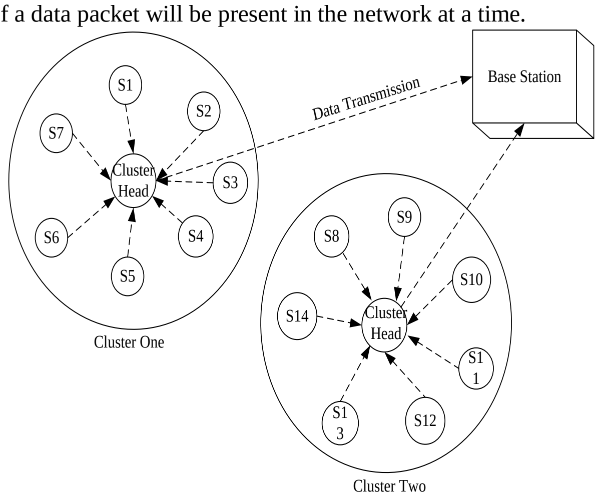

Fig 4: Clustering Techniques between sensor nodes and Sink/Base Station in WSN

There are others routing mechanisms such as partial flooding and multipath routing scheme. It has been observed in past studies that single path routing schemes can save many resources as minimum resources required for the data transmission for this scheme as compared to conventional multipath or flooding-based approaches. In highly dynamic network scenario flooding -based routing achieves better performance and ensures efficient packet delivery services. But various routing protocols which are designed to mitigate various routing issues can also be affected by various malicious attacks such as bogus routing information, Selective forwarding, and Sinkhole attack, Hello flood attack, Wormhole attack etc. Various constraints present in the existing routing protocols are discussed below.

Limitations and Challenges associated with various existing protocols

- Lack of security mechanisms in SPIN Protocol
- Detection of malicious nodes and secure route formation
- Recovery of damages caused by compromised nodes.
- Issues of notation which is associated with a trade-off between security and communication cost.
- Lack of security in multipath routing.

3. SECURITY VULNERABILITIES IN WSN

In WSN, all the nodes are self-configured as an example it can be said that all the nodes in a particular area can be connected with each other in an Ad hoc manner without the presence of internet connectivity. This self-configurable characteristic causes the vulnerabilities in wireless sensor network, where a node which has been deployed by an intruder within the network can act as a genuine node and drop all the data packets which are passing through it. Discussion of various attacks can be seen in Fig.5. For optimizing this issue various authentication mechanisms, have been introduced for considering a genuine node to be a part of the route. Current Wireless sensor network organization is susceptible to cause the physical harm of the network by introducing two different types of attacks: Active Attacks and Passive Attacks. Active Attack is a threat caused by the misbehaving nodes which can carry some energy costs to perform the disruption [6]. On the other hand, passive attacks are mainly improvised to avoid the coordination between nodes with a purpose to store up or save the energies regardless of other nodes. Nodes are considered to be malicious if they are aiming to damage the other nodes by network outage and nodes which are responsible for making passive attacks to save the consumption of their power source for their own communication purpose are determined to be selfish nodes. Different types of attacks are classified in the basis of modification, personification, fabrication wormhole and lack of cooperation some of the significant attacks are shown in the diagram below.

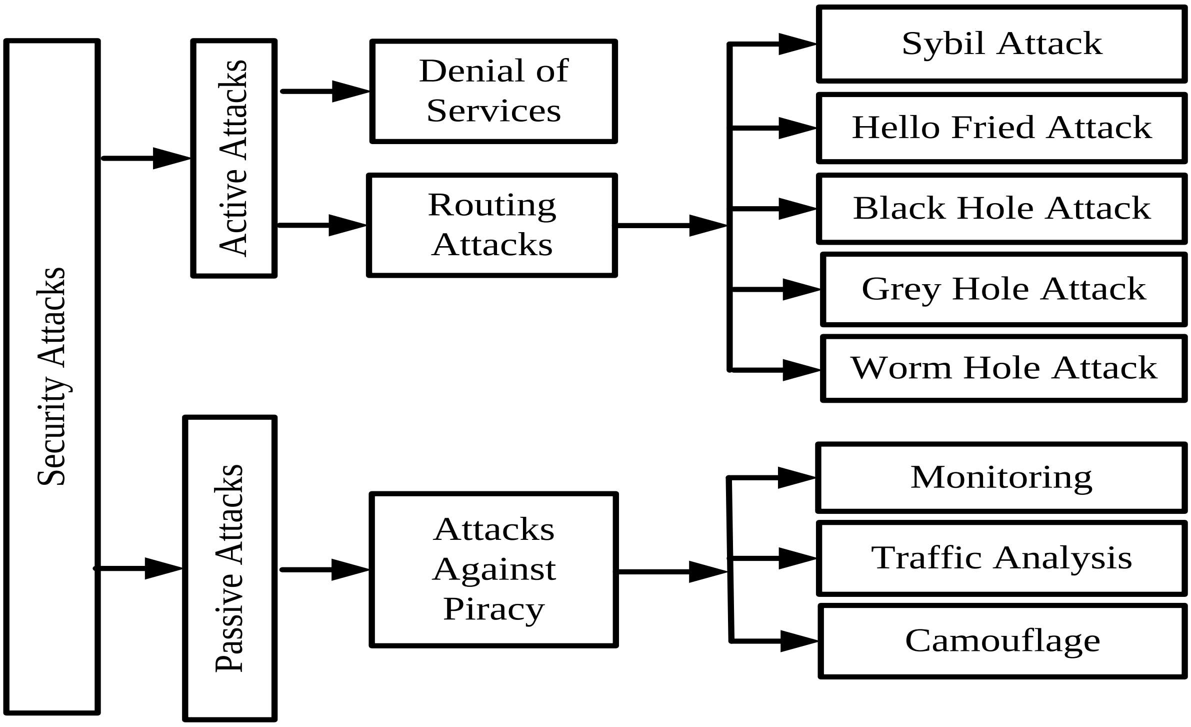

Fig 5: Various security attacks on wireless sensor network

The following Table 1 highlights discussion of various attacks on wireless sensor network where it has been shown the severity and vulnerability of various attacks on the network. Brief discussion and effects of the various attacks will be quite helpful for the future researchers for overcoming various security issues associated with WSN.

Table.1: A comparative analysis of various attacks on WSN is highlighted

Attacks	Brief Discussion	Effects On The Network	Criticality
Eavesdropping	Overhearing The Communication Channel For Collecting Some Private Data.	• Reduces Data Privacy Extract Virus-Related Information	Low
Traffic Analysis	Computing Parameters That Responsible For Affecting The Network Traffic.	• Increase Packet Collision • Traffic Distortion	Low
Camuflage	Malicious Nodes Acts As A Normal Node	• False Data In Network • Increase Packet Loss	Low
Sybil	Pretense From Multiple Malicious Nodes With Multiple Fake Identities For Attacking Data Packets.	• False Sensor Readings • Increase Packet Loss	High
Blackhole	Attacks All Possible Traffic Routes.	• Modification Of Route Information Corruption Of Data	High
Denial Of Services	Stops Users For Getting Access To The Network.	• Reduces WSN Availability	High
Wormhole	Tunneling From One Location To Another	• Modification Of Normal Message Streams	High
Hello Flood	Abnormal High Transmission Power Transmit The Messages From Malicious Nodes.	• Packet Loss • Route Disruption	High
Grey Hole	Selective Dropping Of Data Packets.	• Packet Loss • Information Modification	High

This study is more focused towards the detail analysis of various existing secure routing techniques of wireless Sensor Networks and gives a brief overview of various malicious attacks and their Severity in the area wireless sensor network which is discussed in the Table I. The proposed study also discusses about the review of literature and the research gap found in the two decade investigation towards various techniques which have been introduced for mitigating the various routing attacks of wireless sensor network. Conclusion and the future work are highlighted in the end of the paper. The main contribution of this paper is the research gap and the further direction of the research.

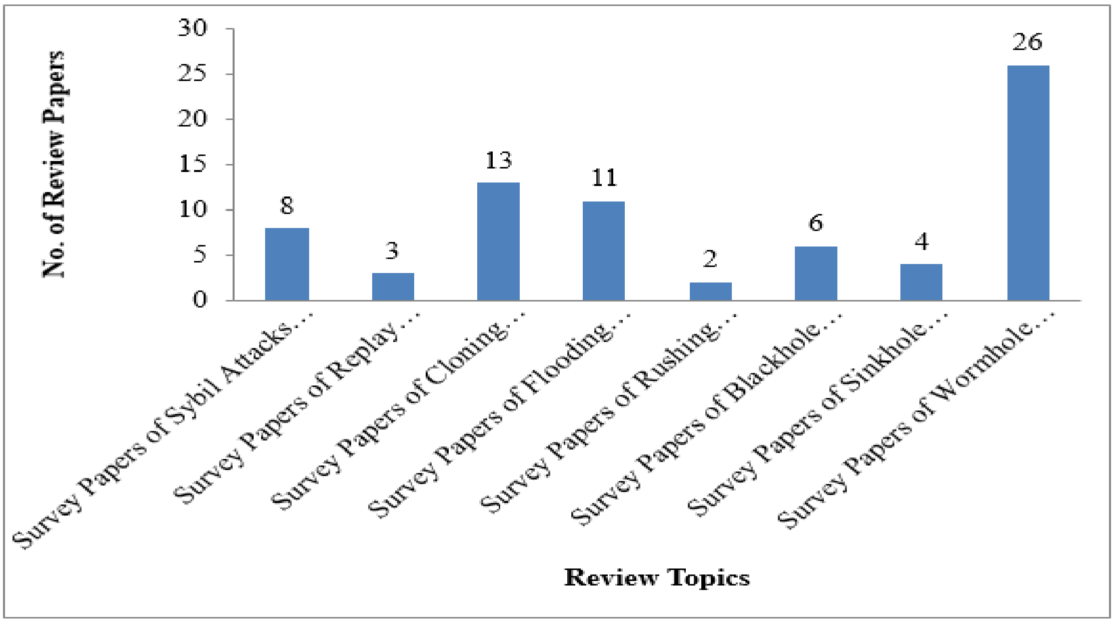

Fig 6: Statistics of Survey on Various attacks of Wireless Sensor Network (2004-2014)

4. RECENT SURVEY STUDIES

This section gives an overview about the various existing review studies associated with vulnerable attacks of Wireless Sensor Network. It is found in the website of IEEE Explorer , with the search keyword “Attacks on WSN” The web server returns Content types including 1953 Conference publications , 254 journals and magazines , Early access article and books 17 and 6 respectively. And total 7 open access journals and magazines are found which talks about attacks of WSN in IEEE Explorer within the range of 2008 to 2014. Fig 6. Shows the statistics of the Various Attacks of Wireless sensor network whereas Fig 7 talks about the various attacks of MANET within the range in between 2004 – 2014. It has been found in the recent survey studies that most of the existing review works mainly focuses on wormhole attacks with respect to WSN as well as MANET. Fig 6 shows that survey papers on worm whole attack are more as per the information given by the statistics where as it has been seen that in the area of MANET, majority of the papers focuses on Black hole attacks rather than wormhole attacks. There are various papers indexed in the IEEE Explorer also discusses about various attacks such as flooding (DoS) , rushing attack , Grey hole attack , traffic analysis , sink hole attacks both on MANET and WSN. Table-2 reviews the most recent survey papers on WSN which will be beneficial to draw the attention of the future researchers. The prime aim of the proposed survey study is to discuss about the significant findings of attacks associated with WSN and their prevention techniques. After evaluating the existing studies the research gap of the various existing secure routing techniques have discussed in the section IV.

Table.2 Summery of Existing Survey Papers

Authors	Year	Topic on Focus	Inference
Nagrath et al [7]	2011	Wormhole Attack	**Pros**: Good Theoretical Discussion on Domain **Cons**: No discussion about the prior implementation.
Terence et al [8]	2011	Wormhole attacks in Sensor Network.	**Pros**: Discussed various techniques. **Cons**: Extremely narrowed discussion about various techniques.
Gelenbe et al [9]	2012	Wireless Sensor Assisted EMS	**Pros**: Good theory about routing **Cons**: Most of the part of discussion is repetitive in nature.
Almeheiri et al [10]	2013	Sensor Network Protocols	**Pros**: Discussed Prior techniques **Cons**: No Statistical Analysis in terms of existing studies.
Chila et al [11]	2013	Secure Routing of WSN.	**Pros**: Good theory on domain **Cons**: Narrowed discussion about prior studies.
Sowmya et al [12]	2014	Jamming Attacks on WSN	**Pros**: Good Theoretical discussion on Jamming Attacks of wireless network. **Cons**: Comparison and analysis has not been highlighted.
Dhanalaksmi et al [13]	2014	Sybil Attacks on WSN	**Pros**: Acceptable Discussion on Domain **Cons**: Brief Survey of Attacks.
Alheeti et al [14]	2014	Attacks on WSN	**Pros**: Discussed only few techniques **Cons**: No discussion about the research gap.
Autkaar et al [15]	2015	Node Clone Detection in WSN	**Pros**: Good Review discussion about existing studies. **Cons**: Repetitive discussion about prime implemented techniques.

5. RELATED WORK

Although various routing protocol designs have been planned in the field of wireless sensor networks for addressing the security issues but some of the proposed techniques are not directly applicable in the domain as they have some constraints. This section talks about various existing significant protocols in brief. The study of Liu et al [16] designed a secret distribution based multipath routing algorithm as an optimization problem where the study aims to maximize both the network security and life time for wireless sensor network. A three phase disjoint routing scheme has been proposed which is based on the secret sharing algorithm. The performance analysis and the simulation results demonstrate the effectiveness of the proposed system. BIOSARP a secure routing protocol also proposed by Saleem et al [17] where an architecture, implementation and detailed experimental outcomes of proposed BIOSARP are presented. The comparative analysis and the experimental outcomes show the BIOSARP improves the energy efficient ant-based routing. Ganesh et al [18] modified the ad-hoc which is based on demand distance vector routing by including the signal to noise ratio based on clustering technique. The proposed mechanism poses efficiency in secure routing in wireless sensor networks with the help of SNR-based dynamic clustering (ESRPSDC) mechanisms. Nodes can be portioned into clusters by the proposed scheme. The performance analysis of the proposed system shows the hybrid ESRP significantly achieve better energy efficiency and the packet delivery ratio. It has been observed in the work of Ruj et al [19] where pairwise and triple key founding glitches are found to be addressed in wireless sensor networks. And several types of designs have been introduced. The functionality of the proposed scheme has been extended and applied to the secure data aggregation. Jungi et al [20] proposed an energy aware trust derivation mechanism which is based on the game theoretical approach which manages overhead in the time of maintenance of security. The game theoretic approach is applied in the trust deviation process for reducing the overhead of the process. A differentiated hey distribution method has been used by Gu et al [21] for designing an end to end secure communication protocol. The performance analysis shows the effectiveness of the proposed system. The work proposed by Zhan et al [22] presented a TARF a robust trust aware routing outline for the dynamic environment of wireless sensor network. The Comparative analysis also has been done to provide the effectiveness. The study of Lazos et al [23] proposed a range independent localization algorithm which is called high resolution range independent localization protocol that permits sensors to passively detect their location with high resolution. Li et al [24] an evaluation metric path vacant ratio is proposed for evaluating link disjoint paths to the destination depending on path vacant ratio. Simulations have been done with various performance parameters. A secure based loose synchronization protocol has been designed by Uluagac et al [25] to secure the synchronization of various events in the wireless sensor network. Both analytical a simulation result shows that the proposed scheme have been verified carefully under normal operation and various malicious attacks of the network.

6. RESEARCH GAP

Following discussion highlights the Research Gap after reviewing the existing studies towards Attacks of wireless Sensor Network.

i) Narrowed Survey: The summery of existing survey papers which have been published in between 2011 and 2015 has been briefly highlighted and reviewed in table 2. It has been observed that majority of the existing studies till date only discusses the theoretical background of the various attacks. Most of the survey works indexed in IEEE Explorer are repetitive in nature. Almost All the existing review papers hardly discusses about the prevention techniques oriented with the various malicious attacks of Wireless Sensor Network. In the existing review papers the better classification of studies are significantly missing thus poor discussion of existing techniques in terms of parameters do not provide a better resolution or scope towards research direction. The comparative analysis of the various techniques with respect to benchmark paper is very much crucial as it contribute the reader a better understanding of the efficient existing techniques till date. It has been also found that majority of the existing techniques uses the repetitive mathematical modelling. Majority of the contents of the existing review papers are repetitive in nature with other survey papers and no significant outcomes could be derived after gathering or reading the survey papers.

ii) Few Benchmark Studies: From the information which has been provided by the related work section, it can be seen that the majority of the existing studies such as [18] [19] [20] [22] are not bench marked at all. As a result it will be difficult for the reader to understand the efficient secure routing technique for prevention of various vulnerable attacks performed in the wireless Sensor Network and as some critical information are missing from the above mentioned studies so that the concept of those technique will not be adopt by the future researchers.

iii) Repetitive Nature of Implementation: After revising so many papers which are included in the proposed study it has been found that most of the existing studies related to secure routing in wireless sensor networks which implements and analyses new routing protocols for the prevention of various routing attacks in WSN are repetitive in nature. Better Comparative Analysis of the existing studies with respect to the proposed techniques and various performance parameters are significantly missing. As the comparative analysis with respect to various performance parameters are very much essential for the for the reader to understand the most efficient techniques till date which assist the reader to continue the further research for mitigating the various issues related to that domain. No significant outcomes could be resulted after reviewing the existing studies where the repetitive nature of implementations has been adopted. Few benchmarked studies have been found as the majority of the papers highlighted in IEEE Xplorer are not benchmarked at all. This situation creates a very much challenging environment for the readers to understand the reliability of the various existing studies towards secure routing techniques of wireless sensor network.

iv) Less effective Performance parameters: Selection of performance parameters also play important roles in the field of secure routing for Wireless Sensor Networks whereas majority of proposed papers highlighted in IEEE Xplorer use very less effective and repetitive performance parameters as it is very crucial for understanding of the performance metrics of the proposed system with respect to the benchmark study.

v) Further Directions of the Research: Some limitations arise in the field of multi-hop routing where some of the base stations consists of one or two hop connections and easily can be compromised by the intruders. These characteristics of the Sensor Networks can be optimize by clustering protocols such as LEACH which constitutes the optimization of communication overhead between links and provide the secure routing of data packets from cluster heads to base stations. The proposed study has focused on presenting comparative analysis of the existing routing schemes which are still vulnerable to various routing attacks. Only the Link layer encryption and authentication techniques do not give better solution for preventing various routing attacks where the careful design of routing protocol does. These constraints associated with the design issues of routing protocols of WSN have been considered as an open issue for future research direction.

7. CONCLUSION

WSN is one of the most preferred topic in advanced networking owing to the potential advantages of cost effectiveness in communication system. Hence, such forms of network should be free from majority of the lethal threats. However, from past decades there are evidences of various literatures that shows that security factor is one of the most frequently research topic and till date there are few security protocols that offers sustainable and robust security-enabled services in time-critical applications of WSN. Various challenges come out from the applications of wireless sensor networks, but this proposed study gives more attention on security aspects which are associated with the wireless sensor networks to mitigate various susceptible attacks performed by intruders. The uniqueness of this paper is that this paper gives an overview of various existing routing techniques and highlights most of the significant findings of existing studies. The paper also highlights most of the significant research issues associated with the existing techniques. This survey will be beneficial for the further progress and enhancement of the security techniques for WSN.

8. REFERENCES

[1] Krco, S.; Tsiatsis, V.; Matusikova, K.; Johansson, M.; Cubic, I.; Glitho, R.2007. Mobile Network Supported Wireless Sensor Network Services. Mobile Adhoc and Sensor Systems, MASS, IEEE International Conference, pp.-3

[2] Modares, H.; Salleh, R.; Moravejosharieh, A.2011. Overview of Security Issues in Wireless Sensor Networks. Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference, pp.308-311

[3] Rout, R.R.; Ghosh, S.K.; Chakrabarti, S.2010. A Network Coding based Probabilistic Routing scheme for Wireless Sensor Network. Wireless Communication and Sensor Networks (WCSN), Sixth International Conference, pp.1-6, 15-19

[4] Sutar, U.S.; Bodhe, S.K.2010. Energy efficient topology control algorithm for multi-hop ad-hoc wireless sensor network. Computer Science and Information Technology (ICCSIT), 3rd IEEE International Conference, pp.418-421

[5] Mittal, R.; Bhatia, M.P.S.2010. Wireless sensor networks for monitoring the environmental activities. Computational Intelligence and Computing Research (ICCIC), IEEE International Conference, pp.1-5

[6] Soo-Hwan Choi; Byung-Kug Kim; Jinwoo Park; Chul-Hee Kang; Doo-Seop Eom.2004.An implementation of wireless sensor network," Consumer Electronics, IEEE Transactions, Vol.50, No.1, pp.236-244

[7] Nagrath, P.; Gupta, B.2011. Wormhole attacks in wireless adhoc networks and their counter measurements: A survey," Electronics Computer Technology (ICECT), 2011 3rd International Conference, Vol.6, pp.245-250

[8] Terence, J.S.2011. Secure route discovery against wormhole attacks in sensor networks using mobile agents, Trendz in Information Sciences and Computing (TISC), 2011 3rd International Conference pp.110-115

[9] Gelenbe, E.; Gorbil, G.; Fang-Jing Wu. 2012. Emergency Cyber-Physical-Human Systems. Computer Communications and Networks (ICCCN), 1st International Conference, pp.1-7

[10] AlMheiri, S.M.; AlQamzi, H.S.2013. Data link layer security protocols in Wireless Sensor Networks: A survey. Networking, Sensing and Control (ICNSC), 10th IEEE International Conference, pp.312-317

[11] Wei-Chia Lai; Ying-Ying Su; Chih-Ming Lee; Shih-Hau Fang; Wan-Jung Lin; Xu-Peng He; Kun-Chi Feng. 2013.A survey of secure fingerprinting localization in wireless local area networks. Machine Learning and Cybernetics (ICMLC), 2013 International Conference, Vol.03, pp.1413-1417

[12] Sowmya, S.; Malarchelvi, P.D.S.K.2014.A survey of jamming attack prevention techniques in wireless networks. Information Communication and Embedded Systems (ICICES), 2014 International Conference, pp.1-4

[13] Dhanalakshmi, T.G.; Bharathi, N.; Monisha, M.2014. Safety concerns of Sybil attack in WSN," Science Engineering and Management Research (ICSEMR), International Conference, pp.1-4

[14] Ali Alheeti, K.M.; Ehsan, S.; McDonald-Maier, K.D.2014. An Assessment of Recent Attacks on Specific Embedded Systems. Emerging Security Technologies (EST), 2014 Fifth International Conference, pp.88-93

[15] Autkar, Shriya V.; Dhage, M.R.; Bholane, S.P.2015. A survey on distributed techniques for detection of node clones in Wireless Sensor Networks. Pervasive Computing (ICPC), 2015 International Conference, pp.1-4

[16] Liu, A., Zheng, Z., Zhang, C., Chen, Z., Shen, X.2012. Secure and Energy-Efficient Disjoint Multipath Routing for WSNs. Vehicular Technology, IEEE Transactions, Vol.61, No.7, pp.3255-3265

[17] Saleem, K., Fisal, N., Muhtadi, A. 2014. Empirical Studies of Bio-Inspired Self-Organized Secure Autonomous Routing Protocol. Sensors Journal, IEEE, Vol.14, No.7, pp.2232-2239

[18] Ganesh, S., Amutha, R.2013. Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms.Communications and Networks, Journal, Vol.15, No.4, pp.422- 429

[19] Ruj, S., Nayak, A., Stojmenovic, I.2013. Pair wise and Triple Key Distribution in Wireless Sensor Networks with Applications. Computers, IEEE Transactions, Vol.62, No.11, pp.2224-2237

[20] Duan, J., Gao, D., Yang, D., Foh, C. H., Hen, H-H.2014. An Energy-Aware Trust Derivation Scheme with Game Theoretic Approach in Wireless Sensor Networks for IoT Applications. Internet of Things Journal, Vol.1, No.1, pp.58-69

[21] Wenjun, G., Dutta, N., Chellappan, S., Bai, X.2011. Providing End-to-End Secure Communications in Wireless Sensor Networks. Network and Service Management, IEEE Transactions, Vol.8, No.3, pp.205-218

[22] Guoxing, Z., Shi, W., Deng, J.2012. Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs. Dependable and Secure Computing, IEEE Transactions, Vol.9, No.2, pp.184-197

[23] Lazos, L., Poovendran, R.2006. HiRLoc: high-resolution robust localization for wireless sensor networks. Selected Areas in Communications, IEEE Journal, Vol.24, No.2, pp.233-246

[24] Shancang, L., Zhao, S., Wang, X., Zhang, K., Li, L.2014. Adaptive and Secure Load-Balancing Routing Protocol for Service-Oriented Wireless Sensor Networks, Systems Journal, IEEE , Vol.8, No.3, pp.858-867

[25] Uluagac, S., Beyah, R.A., Copeland, J.A.2013. Secure Source-Based Loose Synchronization (SOBAS) for Wireless Sensor Networks. Parallel and Distributed Systems, IEEE Transaction, Vol.24, No.4, pp.803-813