IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 4, April 2016

Comparative Analysis of Routing Protocols and Security Threats in Wireless Sensor Networks

Ridhi Bhatla[1], Ashok Kumar[2], Preeti Khera[3]

Dept. of Electronics & Communication Engg., Ambala College of Engineering Applied Research, Ambala, India[1,2,3]

Abstract: Wireless Sensor Network is a rising innovation. Wireless sensor networks are more reasonable and capable comprise of bits generally called sensor nodes. One of the real challenges wireless sensor system confront today is security. Security has transformed into a major issues in WSN's since they are effortlessly vulnerable to a greater number of attacks than wired networks, so there's the need for successful security mechanism. This paper thinks about the security attacks, security related issues and challenges in wireless sensor system are examined . Moreover, we give a brief dialog on the not so distant future examination course in wireless sensor system.

Keywords: WSN, routing protocols, challenges, security.

I. INTRODUCTION

With the progression of developing Wireless sensor system in Micro-Electro-Mechanical systems (MEMS) – based sensor innovation is a low power automated contraptions conceivable to create wireless sensor nodes in amount at low cost [1].sensor nodes are multifunctional small nodes capacity to perform sensing, processing of information and comprise of conveying components. WSN are sent in extensive variety of applications for instance health, environmental, military, home and other commercial applications [2]. The sensor nodes are usually strewn in sensor fields as shown in Fig.1.

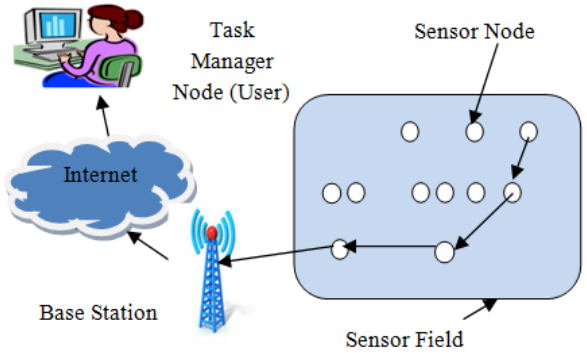

Fig.1. Architecture of Wireless sensor Network

The WSN is made by few and in addition an extensive number of sensor nodes, where every hub is associated with one or some of the time a few sensors. Every sensor system hub has normally a few parts: a radio trans receiver by having an interior reception apparatus or join with an extra receiving wire, a microcontroller, an electric circuit for interfacing with the sensors and a power source (i.e. battery or an inserted sort of vitality reaping).WSN's topology varies from far ward mesh network to an enhanced multihop wireless mesh network. Routing and Flooding can be used as propagation techniques. Each Sensor nodes consist of various sensors are also called motes and have capabilities of collecting data and route back data back to the sink . Sink is considered as node which communicate with a task manager node(user) via satellite or Internet which performs data storage ,analysis and display. Sensor nodes performs sensing, computing and consist of communicating constituent which describes the architectural feature of wireless Sensor Network.

Necessity of Wireless Sensor Network: To design a network we consider many design factors for efficient deployment are:

Reliability- It is the power of the network for reliable data transmission in network structure that lead to continuous change it.

Mobility- It is the power of the network to deal with mobile nodes and changeable data paths.

Scalability- It is the power of a network to manage an expanding level of work in a capable way or its ability to be extended to take into consideration that development.

Responsiveness- The power of the network to rapidly adjust itself to changes in topology.

Production Cost- It is a total expense involved in the deployment.

Challenges of Wireless Sensor Network: The various challenges faced in Wireless Sensor Network are:

- Less power consumption
- Network Lifetime should be increased as sensor nodes should die quickly.
- Cost and expense on the network should be less.
- High security Mechanism is required.
- Heterogeneity of nodes.
- Survival in adverse harmful conditions.
- Less Prone to communication failures.

These are some challenges of WSN's to achieve realibility and efficiency of the system.

Section II made comprehensive survey i.e. literature survey. Section III describes various Routing Protocols. Security Threats are discussed in Section IV followed by conclusion and References.

II. LITERATURE SURVEY

K. Sohrabi, et al.[2] had presented their state of the art of wireless sensor networks, its design features and

architecture. Challenges and various Routing Protocols are also discussed. Several Research issues and open challenges are also discussed. I. Akyildiz et al. [3] had exhibited an intensive review of the late writing on different regions of WSNs and discussed how a wireless sensor network works and discussed advantages and disadvantages inside of the customary network. Wendi B. Heinzelman *et al.* [4] had developed and analyzed clustered based low-energy adaptive clustering hierarchy (LEACH), an efficient protocol architecture for sensor networks that consolidates the idea of energy efficient routing with applied data aggregation to achieve efficient performance in terms of system lifetime, reliability and application perceived superiority. Lindsey et al. [5] proposed PEGASIS which was an optimal chain based protocol that was undeniably an immense improvement over LEACH. In PEGASIS each node communicates simply with a neighbor and transmits to the base station in turns thus reducing the sheer numbers of energy spent per number of rounds. Simulation results provided by them showed that PEGASIS performed superior than LEACH by around 100 to 300% when 1%, 20%, 50% and 100% of nodes pass away a variety of network sizes and topologies. PEGASIS showed a little bit more enhancement as the network size increases. Cai et al. [6] verified an adaptive method to detecting black and grey hole attacks in ad hoc network with different cross layer design. They proposed a path-based approach in network layer to eavesdrop on the next hop's action. They chose DSR protocol to check algorithm and uses ns-2 as simulation tool. Their experiment result verifies that standard detection minute rates are above 90% as well as false positive minute rates are below 10%. Moreover, the adaptive threshold strategy resulted in lowering the false positive rate. Parul Tyagi *et al.* [7] analyzed recent routing protocols for wireless sensor network and characterize in three types of methodologies as per network construction modeling in WSN i.e. Flat, Hierarchical and location based routing protocols. They additionally concentrate on communication overhead savings in each routing protocols and performance issues of routing techniques are discussed. Yusnani Mohd Yussoff *et al.* [8] presented the survey on physical attacks accompanied with ensured memory that not only secure sensor hub's delicate accreditations but rather give a solid system to trust nodes in the committed wireless sensor network. Likewise rundown of proposed IBE_Trust structure is exhibited and quickly examined. Aashima Singla *et al.* [9] had shown concerned about security in sensor network, security issues and DoS attacks on different layers. They discussed various parameters that are required of security (availability, integrity, confidentiality and authenticity) that can be directed by different physical attacks. Gondwal et al. [10] proposed a technique which involves a use of check agent based technology and multiple base stations to detect blackhole attack. This technique reduces message complexity and increases energy efficiency. In this multiple base stations are used thus ensuring success of high packet delivery reaching atleast one base station. The proposed technique is further competent than the prior techniques and gives improved results. Zhao Han *et al.* [11] proposed a General Self Organized Tree- Based Energy-Balance routing protocol (GSTEB) which accumulates a routing tree utilizing a method where, for each round, BS assigns a root node and broadcasts this selection to all sensor nodes. Subsequently, each node selects its parent by taking into consideration only itself and its neighbours information, thus creating GSTEB a efficient protocol. They show GSTEB has a better performance than other protocols in balancing energy consumption, thus improved the lifetime hence provides better security than any other existing routing protocol.

III. ROUTING PROTOCOLS IN WSN

In Wireless Sensor Network, the sensor nodes are more vulnerable to problems such as packet loss, limited lifetime, more power consumption. As a result Nodes dies quickly. To overcome these problem so as to achieve increased lifetime and energy efficiency of the nodes we need some powerful protocols that overcome the challenges we faced such as fault tolerance, scalability, production cost ,QOS, accuracy and power consumption are some aspects taken into consideration. Conventional Routing is different from routing in WSN's as this do not have proper infrastructure, wireless links are not predicted and can be stop working in harsh environments. Many routing algorithms [2] were proposed for wireless sensor networks. All major Routing protocols are classified into three main categories:

- Location based Protocols
- Data Centric Protocols
- Hierarchical Protocols

Routing protocols classification can be shown in Fig 2 that are useful in increasing reliability and system efficiency can be shown as:

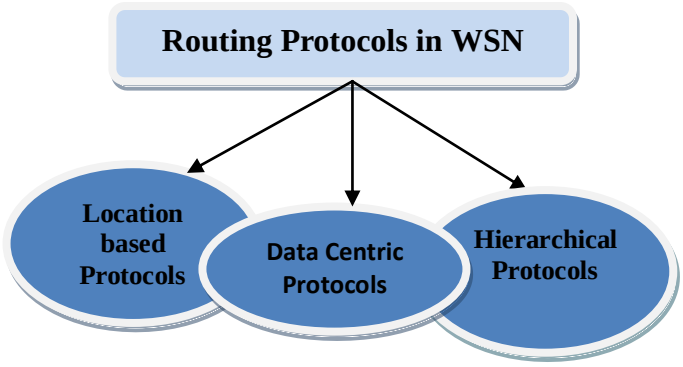

Fig.2. Classification of Routing Protocols for Wireless Sensor Network

A. Location Based Protocol

The location information based routing protocol utilizes location information to guide routing disclosure and maintenance as well as data sending, empowering directional transmission of the data and maintaining a strategic distance from data flooding in the whole network [7]. Location information is required in order to compute the distance between two specific nodes so that energy utilization can be assessed. These Location based Protocols were further divided into major categories as shown in Fig. 3.

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 4, April 2016

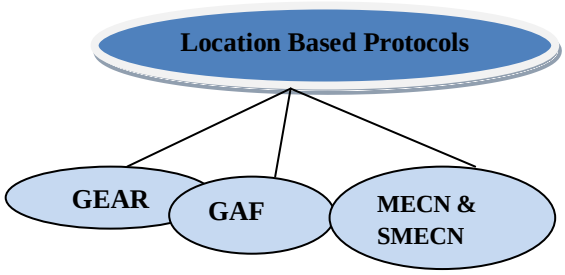

Fig.3. Classification of Location Based Protocols

Some important Location Based Protocols that can be widely used are:

i) GEAR

GEAR (Geographic Energy Aware Routing) is an algorithm in which each node keeps an expected cost and an understanding expense of accomplishing the destination through neighbours. The assessed cost is an assortment of residual energy and separation to destination. Occurrence of hole each time a node does have no closer neighbours to the target. If no holes are founded, the evaluated cost adds up to the area cost. The area expense is propagated one hop back every time a packet achieves the destination to ensure that route make for next packet is prone to be balanced.

ii) GAF

Geographic Adaptive Fidelity (GAF) is utilized for WSN as Energy conservation is favoured.GAF consists of state transition states which were further divided into three stages; Active, Sleeping and Discovery. When sensors enters the sleeping mode, radio is turned off power saving mode. In Active state, discovery messages are periodically broadcasted by the sensors that help in investigation of similar sensors. In discovery stage, discovery messages are exchanged to see same sensors about its state. State Transition stages of GAF are shown in Fig.4.

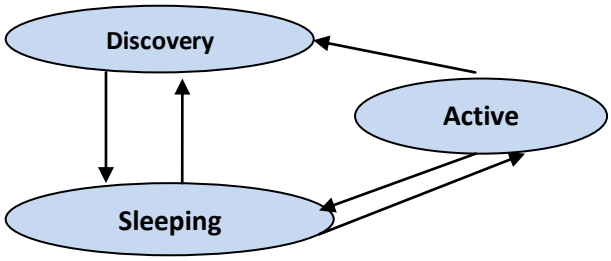

Fig. 4. Stages of State Transition of GAF

GAF thus helps in saving the battery power and reduce number of nodes to make a network.

iii) MECN and SMECN

MECN i.e., Minimum Energy Communication Network creates wireless network which has very least energy and maintains low power GPS utilization. It is better applicable to non mobile sensor networks. The key target of MECN is to discover sub network which has less number of nodes and less power utilized for transmission between two particular nodes. Hence, by not considering most of the nodes in the network global minimum power paths are observed. SMECN i.e., Small Minimum Energy Communication Network is an expansion to MECN.

MECN	SMECN
Each node can transmit to every other node which is not possible at every instant of time.	Between any sets of nodes possible obstacles are considered at every instant of time.
Whole Network may be remained as fully connected.	Sub Network is constructed first than main network is constructed in this case

Table1. Difference Between MECN and SMECN

Hence, SMECN utilizes less Energy and Maintainance cost of links between them.

B. Data Centric Protocols

In Data Centric Routing, data has given more importance than sensors nodes itself. Rather than actual data it carries aggregated data and data carried by this differ from the data carried by traditional centric protocols [3]. The main examples of Data Centric Protocols as shown in Fig. 5.

i) SPIN

SPIN i.e. Sensor Protocol for Information via Negotiation is Data centric protocol that effectively disseminate data among sensors in an energy-constrained wireless sensor network and overcome the issue of implosion and in classic flooding overlap happened. Negotiation guarantees that the transmission of redundant data throughout the network is eliminated and only valuable data will be transferred.

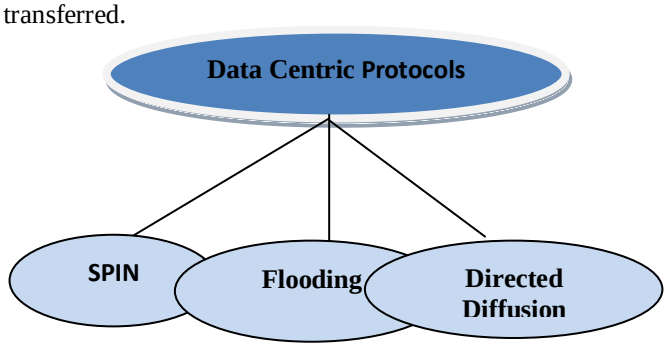

Fig. 5. Examples of Data Centric Protocols

It decreases energy consumption by a factor of 3.5 as compared to flooding. The disadvantage of SPIN protocol is it is uncertain about the data will achieve the target or not and can also be bad for high-density distribution of nodes. Therefore, SPIN isn't a great decision for applications.

ii) Flooding and Gossiping

Flooding is also a traditional method which is used for routing in WSN's. In this Data is relayed in sensor network without necessity of topology maintenance and algorithm [3]. Flooding suffers from drawbacks such as implosion problem, Resource Blinding and overlapping. Gossiping is enhanced version of flooding as in this data is randomly send with the help of nodes and hence avoids the implosion problem.

iii) Directed Diffusion

It is favoured data total paradigm for wireless Sensor Network called Directed Diffusion. All the nodes in this are application aware. To attain energy saving it enables diffusion by selecting good paths and by caching and by preparing data in the network. It consists of several

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 4, April 2016

elements: Reinforcements, Gradients, data messages and interests. It is not a good choice for application such as monitoring of environment as it requires constant information conveyance to the sink won't work productively with a question driven on demand data model.

C. Hierarchical Protocols

The efficient protocol used in this is clustering that has many advantages over other protocols as it transmits aggregated data into the sink, the number of nodes taking part in transmission is reduced ,energy efficient technique that reduces overhead for both multihop and single hop communication. Hierarchical routing [11] is very efficient Routing that allows capabilities of optimization at the cluster heads. Several clusters are present in one network and each cluster have its own cluster head that provides coordination to the data transmission activities that performed by sensors. Some of the hierarchical protocols used for routings are shown in Fig.6.

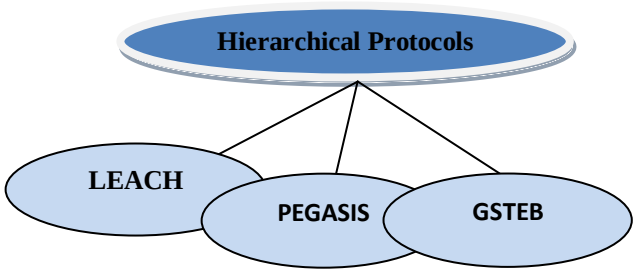

Fig.6.Classification of Hierarchical Protocols

i) LEACH

LEACH (Low Energy Adaptive Clustering Hierarchy) [4] clustered based Routing Protocol which was first proposed for wireless sensor Network to increase the energy efficiency of a system. It comprises of cluster heads that aggregate all the information and nearest base station collects the information. It assumes that each node has sufficient power to reach the base station directly but by applying radio at full power would waste energy. After P rounds cluster heads do not became again an cluster heads. The round when comes to end ,the closer cluster head is chosen by each node which is not a cluster head and combines that cluster to transmit data. Leach is based upon two assumptions:

- All the nodes are homogenous in nature.
- Base station is far away from the location of sensors and is assumed to be fixed.

The operation of Leach protocol is divided into two phases:

- Setup Phase
- Steady State Phase

These phases can further be divided into phase such as advertisement phase in which selection of cluster head takes place. Next is cluster setup phase in which non cluster head send ACK to cluster head so that nodes become member of cluster head to which they belong using CSMA MAC protocol. After cluster set up schedule creation phase takes place in which all the information is clustered together and TDMA schedule is made. After the Cluster Setup and TDMA schedule Data transmission phase takes place in which all the information from the cluster heads are gathered together and further is compressed and send to base station. Hence in this way one phase transmission is completed. This operation is also called steady state phase.

LEACH outperforms good performance but leads to several drawbacks such as

- It can't be suitable for large networks.
- It suffers from 'Hot Spot Problem'.
- Clusters are not fixed.
- It results in long latency.

ii) PEGASIS

PEGASIS (Power Efficient Gathering in Sensor information system) is power efficient algorithm based on Greedy chain concept [5].The air model of PEGASIS is exactly like LEACH protocol. The important features of PEGASIS are:

- Sensor Nodes do not have mobility.
- Base station is fixed from the distance of sensor nodes.
- Sensor nodes are Energy constrained having uniform energy and homogenous in nature.

Chaining and Data Fusion are two concepts on which it is based. In chaining, the chain is constructed using greedy algorithms in which each node will become leader of chain. PEGASIS assumes that sensor nodes have no mobility , nodes have location details about all the nodes, and have international understanding about all the nodes. In Data fusion which acknowledges the data fusion in chains. PEGASIS outperforms LEACH by reducing the overhead information, uses 1 transmission per round. It also suffer same drawback as LEACH that it can't be put on the network where global understanding of network is difficult to achieve.

iii) GSTEB

General self organised tree based routing protocol (GSTEB) [11] is Tree based Routing Protocol aims to provide the extended lifetime for various applications. GSTEB operates in rounds and in each round root node is assigned by the base station and ID of root nodes are broadcasted and coordinate to all the sensor nodes. It may change the basis and routing tree will be reconstructed with low energy consumption and short delay. The operation of GSTEB is divided into four phases:

i) Initial Phase
ii) Tree Constructing Phase
iii) Self-organized data collecting and transmitting phase
iv) Information Exchanging Phase

i) Initial Phase: During the initial phase, packets are broadcasted by the base station to all the nodes and each node send packets in group having particular radius during unique time slot. Neighbours receives the packets and store info in the memory. After Initial phase, it operates in round where each sensor nodes generates data packets that further transferred to base station. All the information of sensor nodes received by the base station, a round finished.

ii) Tree constructing phase: In this phase root is assigned by the base station and a node having greater residual

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 4, April 2016

energy will come root for current round. The energy level of the nodes can be computed by using the function:

$$EL\,[11] = \frac{\text{Residual energy (i)}}{\alpha} \qquad (1)$$

In equation (1), where 'i' may be ID of every node and α is a constant considered as minimum energy unit. Each node knows about all its child nodes. If child nodes are not present, it assumes itself as leaf node from that data transmission begins.

iii) Self-Organized Data Collecting and Transmitting Phase: After the construction of routing tree, all sensor nodes gather the information to produce a data packet which must be transmitted to base station. After receiving all the data from the child nodes, the node itself become leaf node and send fused data in next time slot. To examine communication interference for a parent node initial segment is required. During this interval each leaf node sends a information that contains ID to its parent by assuming the whole energy consumption but not the length.

iv) Information Exchanging Phase: Before the death of each node it must generates data and transferred o the base station. The death of sensor node can affect the topology. So the nodes that are likely to die have to share with other sensor nodes. Root node is selected on the basis of degree of energy so that no delay is observed and information may be transmitted securely. GSTEB outperforms in the entire basis such as extended lifetime, negligible overhead, no hotspot problem, can be put on large areas, no delay is observed hence it is an efficient routing protocol used for routing in wireless sensor networks.

Parameters	LEACH [4]	GSTEB [11]
Data Transmission Model	Cluster Head	Tree Based
Network lifetime	Low	Prolong
Packet Transferred	Low	High
Stability	Low	High
Power Consumption	High	Low
Average Remaining energy	Low	High

Table 2. Comparison of LEACH and GSTEB on the Basis of Performance Metrics[15]

IV. SECURITY THREATS IN WSN

Security is one of the main concern of any communication system. Wireless sensor network consists of limited constrained energy source and hence dissipate power in a short period of time. This makes sensor nodes exposed easily by the attackers by conveying greater number of assets than any other base station which won't not be an difficult work for the attacker. A sensor node is made up of large number of nodes which can be used for multicast and broadcast transmission. Hence due to broadcast nature of wireless sensor network it becomes more prone to security attacks.

These attacks can be classified as:

- Attacks on network Availability
- Attacks on authentication and secrecy
- Attacks on service integrity

Denials of service (DoS) [9] attacks are the attacks on the network availability. DoS attacks degrade the performance of WSN's badly. Various DoS attacks on different layers of the networks are discussed below:

Physical layer: Jamming, Eavesdropping are the major reasons to inject Dos attack in this layer.

Datalink Layer: When attack injected this layer results in collision and Malicious misbehaviour of node is introduced.

Network Layer: This layer is affected by various kinds of attacks such as Sybil, Blackhole, sinkhole, Gray hole that degrade the routing performance of any sensor network.

Transport Layer: It is subjected to session hijacking attack and flooding attacks.

Application Layer: It is subjected to data corruption ,butter overflow, viruses and worms.

Different DoS attacks on the different layers can be classified as [9]:
A. Spoofed, altered, or replayed routing information
B. Jamming
C. Selective forwarding
D. Physical attacks
E. Wormholes
F. Sinkhole attacks
G. Sybil attacks
H. Black hole attacks
I. Gray hole attacks

A. Spoofed, altered, or replayed routing information
In these types of attacks, every node acts as a router and directly affects the routing information. It generates false error data, create routing paths and latency can be increased.

B. Jamming
Jamming is type of attack which occurs on the physical layer of the network. It is destructive in nature and classified as two types intermittent jamming and constant jamming. In intermittent jamming nodes periodically communicates the data not continuously and in constant jamming complete network is obstructed.

C. Selective forwarding
In a selective forwarding attack, malicious nodes selectively drop only certain packets and ensures that they do not propagated any further. In this malicious node just behave like black hole.[10] and will not forward every packet it sees. On network layer it occurs and is possible on Location based routing protocols, Heirarchical protocols, Network flow and QoS aware protocols.

D. Physical Attacks
Physical attacks [8] injected due to distributed nature of deployment of sensor nodes and sensors are destroyed permanently. In this attacker modify the data in the node, cryptographic keys may be extracted, programming of sensors may be modified or replacement of sensor nodes with malicious node can be done.

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 4, Issue 4, April 2016

LAYER	ATTACKS	PROTOCOL
Physical layer	Spoofed , altered or replayed Routing information [6]	Hierarchical
Physical layer	Jamming [6]	Hierarchical ,Flat-routing, Network flow and QoS
Physical layer	Selecting Farwarding [10]	Hierarchical, Flat-routing, Network flow
Physical layer	Physical Attacks [8]	Hierarchical, Flat-routing, Network flow
Network layer	Warmholes [12]	Hierarchical, Flat-routing, Network flow and QoS Aware
Physical layer	Sinkhole [6]	Hierarchical, Flat-routing, Network flow and QoS Aware
Network layer	Sybil [13]	Location based, Heirarchical, Flat-routing
Network layer	Blackhole [10]	Hierarchical, Flat-routing, Location Based, Network flow and QoS Aware
Network layer	Grayhole [6]	Hierarchical, Flat-routing

Table 3. Security Issues on Different Layers in Wireless Sensor Network

PERFORMANCE METRICS	FLAT-BASED/ DATA-CENTRIC ROUTING	LOCATION BASED ROUTING	HIERARCHICAL ROUTING
Structure	Complex query , Event driven	Virtual grid, Demand driven, Continuous	Tree based, Clustered, Chains based
Scheduling	Contention -Based	Contention-Based	Reservation-Based
Overhead	Low	Low	High
Energy Dissipation	Low	Low	High
Latency	High	High	Low
QOS	Nil	Nil	Nil
Query Based	Yes	Yes	No
Examples	SPIN, Flooding, Gossiping	GEAR, GAF	LEACH, PEGASIS,GSTEB

Table 4:Comaparison of Routing protocols[16]

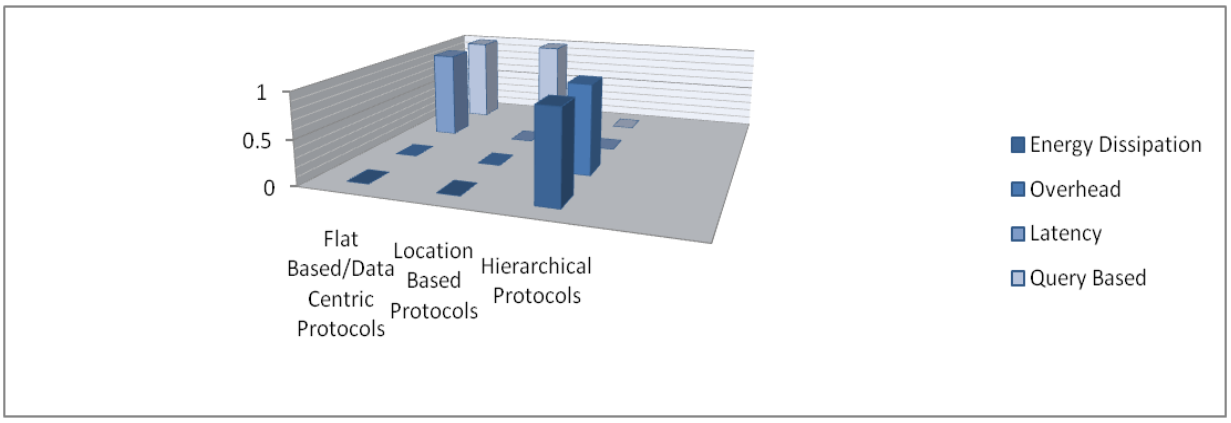

Fig.7: Graphical Representation of Routing Protocols Performance Metrics

E. Wormhole

The Warmhole attack[12], is first detected by the set of bad nodes and record its packets at one location in the network. It act as tunnel between the two parts of network and retransmit these packets again locally. Warmholes are effective even if authenticated or encrypted information is present. This type of attack occurs at initial stages when sensor start to discover the routing information and if it is coupled with Sybil attack and selective forwarding it becomes very difficult to detect.

F. Sinkhole attacks

In a sinkhole attack, the malicious node is present in which always aims to attract all the traffic from a specified area via a compromised node, by making a sinkhole in a centre. This type of attack occurs at network layer. The sinkhole aims to be produced at or near the base station where the traffic intensity is maximum. This kind of attacks occurs in Network flow, QoS, flat based l routing protocols.

G. Sybil attack

In Sybil attack [13], a single node duplicates itself and presents multiple identities to other nodes. Multiple identities are formed by stealing the identity of genuine nodes by falsehood. This attack occurs on network layer and threat to lacation based routing protocols.

H. Blackhole attack

In black hole attack [10], malicious node collects large amount of data and hinders the data to reach the basestation. In this attacker captures the nodes , reprograms them and don't farward the nodes to base station. These reprogrammed nodes are called black hole region.

In Fig. 8 black hole is shown with the black circles and black hole regions are represented by red circles. It first conveys the network that it has highest energy and attracts all the nodes and data from it. After receiving all the data packets, it drops all the packets. This region results in large number of dangerous attacks.

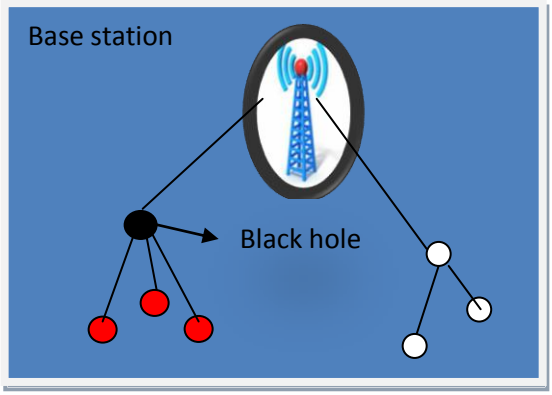

Fig.8.Black Hole Attack [10]

I. Gray hole attack

In Gray Hole attack [6], an attacker node shows its malicious behaviour in several ways and reasonably refuses to send some packets and drops them. It drops all the packets via particular malicious node in the network like black hole attack in first kind. Sometimes, gray hole node drop malicious packets for particular interval of time, but may switch to normal behaviour later.

V. CONCLUSION

In this paper, we present brief overview about wireless Sensor Network, its challenges and characteristics. As the security in the sensor network has become an important issue. So we discussed security issues and DoS attacks such as Black hole attack, Grayhole attack, sinkhole attack. These attacks are possible on all routing protocols. Routing protocols was created to take care of security issues in wireless Sensor Network. This paper do not proposed any new mechanism for packet control. In this comparative analysis of protocols and attacks was studied. Comparison of different security attacks were discussed in Table 3 and comparisons of routing protocols were made in Table 4 and graphical representation was taken out in Fig 7. In future we proposed new mechanisms to overcome challenges by taking different topologies and type of deployment of sensor nodes to improve Energy Efficiency and different performance metrics.

REFERENCES

[1] B.Warneke, K.S.J. Pister, "MEMS for Distributed Wireless Sensor Networks," in Proc. of 9th International Conf. on Electronics, Circuits and Systems, Dubrovnik, Croatia, September, 2002.

[2] K. Sohrabi, et al., "Protocols for Self-organization of A Wireless Sensor Network," IEEE Personal Communications, vol. 7, No. 5, pp. 16-27, October, 2000.

[3] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey On Sensor Networks", IEEE Communications Magazine, vol.40, pp.102-114, 2002.

[4] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy efficient communication protocol for wireless microsensor networks," IEEE Transactions on Wireless Communications vol. 1 (4), pp. 660– 670, 2002.

[5] S. Lindsey, C. S. Raghavendra, "PEGASIS: Power- Efficient Gathering in Sensor Information Systems," presented at Proc. of IEEE Aerospace Conference, Montana, 2002.

[6] J. Cai, P. Yi, J. Chen, Z. Wang, N. Liu, "An adaptive approach to detecting black and gray hole attacks in ad hoc network," IEEE International Conference on Advanced Information networking and Applications, IEEE Computer Society, pp. 775–780, 2010.

[7] Parul Tyagi and Surbhi Jain, "Comparative Study of Routing Protocols in Wireless Sensor Network,"International Journal of Advanced Research in Computer Science and Software Engineering, vol.2, Issue 9, 2012.

[8] Yusnani Mohd Yussoff, Habibah Hashim, Roszainiza Rosli and Mohd Dani Baba, "A Review of Physical Attacks and Trusted Platforms in Wireless Sensor Networks," International Symposium on Robotics and Intelligent Sensors 2012, vol.41, pp.580 – 587, 2012.

[9] Aashima Singla and Ratika Sachdeva, "Review on Security Issues and Attacks in Wireless Sensor Networks," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, Issue 4, 2013.

[10] Nitesh Gondwal and Chander Diwaker, "Detecting Blackhole Attack In Wsn By Check Agent Using Multiple Base Stations," American International Journal of Research in Science, Technology, Engineering & Mathematics, vol. 3(2), pp. 149-152, June-August,2013

[11] Zhao Han, Jie Wu, Jie Zhang, Liefeng Liu, and Kaiyun Tian, "A General Self-Organized Tree-Based Energy Balance Routing Protocol for Wireless Sensor Network," IEEE Transactions On Nuclear Science, vol. 61, No. 2, April 2014.

[12] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002.

[13] J. R. Douceur, "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems, March 2002.

[14] Dheeraj and Ritu Mishra, "Review Paper on Hierarchal Energy-Efficient Protocols in Wireless Sensor Networks," International Journal of Advanced Research in Computer Science and Software Engineering,vol.4,Issue6,2014.

[15] Manjinder Kaur and Dr. Shashi B. Rana, "Performance comparison of Leach and GSTEB in Wireless Sensor Network," International Journal of Engineering Research & Technology, vol. 4,Issue04,2015.

[16] Manjinder Kaur and Dr. Shashi B. Rana, "A study of routing protocols and security threats in Wireless Sensor Network," IRACST – International Journal of Computer Networks and Wireless Communications, vol.5, No.2, 2015.

BIOGRAPHIES

Ridhi Bhatla has done her B.Tech in Electronics Communication engineering from S.D.D.I.E.T, Barwala, PKL,(Haryana), INDIA in year 2014. She is currently pursuing doing her MTech dissertation from Ambala College of Engineering and Applied Research, Ambala (Haryana), INDIA. Her Research interest includes Wireless Sensor Networks.

Ashok Kumar received his M.E. degree in Electronics Product Design and Technology from P.E.C., Chandigarh, Punjab & CDAC, Mohali, India and B.Tech degree in Electronics and Communication Engineering from NIT, Calicut, Kerala, INDIA, and he is persuing Ph.D.(Electronics) from Punjab Technical University, Punjab, India. His employment experience is about 17 years. His research interest includes Wireless Sensor Networks, Digital Signal Processing, Analog System Design and Embedded system Design. He is Head of CREE(Center for Research in Electronics Engineering), ACE and 35 industrial products has been developed under his guidance, he has guided 24 M.Tech thesis and 4 are under guidance, he has published 48 papers in international and national conferences. He is working as Head , Electronics and Communication Engineering Department, Ambala College of Engineering and Applied Research, Ambala (Haryana), INDIA. He is life fellow member of Electronics and Telecommunication Engineering**.**

Preeti Khera received her B.Tech Degree in Electronics and Communication Engineering from Ambala College of Engineering and Applied Research, Ambala (Haryana), INDIA and her M.Tech Degree in Electronics and Communication Engineering from BBSBEC, Fatehgarh Sahib, Punjab,INDIA. Her research interests include wireless sensor networks, Communication Systems and Digital System design. She has published 10 papers in international journals, International and National conferences. She is working as Sr. Assistant Professor, Electronics and Communication Engineering Department, Ambala College of Engineering. and Applied Research, Ambala (Haryana), India

DOI 10.17148/IJIREEICE.2016.4423