ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Visit: www.ijirset.com*

**Vol. 8, Issue 5, May 2019**

# A Review on Layered & Cross Layer Design Issues and Security Attacks in Wireless Sensor Networks

Mrs.Sumalatha M S[1], Dr.V Nandalal[2], Mr.C Santhosh Kumar[3], Mr. V.Anand Kumar[4]

Research Scholar, Department of Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India [1],

Associate Professor, Department of Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India [2],

Demonstrator, Department of Electrical and Electronics Engineering, N S S Polytechnic College ,Pandalam, Pathanamthitta, Kerala, India [3]

Assistant Professor, Sri Eshwar College of Engineering, Coimbatore, India[4]

**ABSTRACT**: Wireless sensor network (WSN) is a wireless network where sensor nodes are spatially distributed. These nodes consist of several technical components like radio, battery microcontroller analog circuits and sensor interface. These nodes are capable to collect the sensitive information like temperature pressure etc. The data collected by these nodes are very sensitive and are vulnerable to many kinds of attacks therefore very much importance must be given while considering the security of these devices. While considering the security of WSN there are two types of approaches are possible. They are layered approach and cross layered approach. This survey paper describes certain investigation about the layered and cross layered communication approach, various WSN attacks and various security techniques etc.

**KEYWORDS:** Wireless Sensor Network, Security, Attacks, Sybil attack.

## I. INTRODUCTION

Wireless sensor network [1-3] is an emerging technology which can be applied for various applications both for mass public and military. The sensing technology of a sensor combined with security, processing power and wireless communication makes it highly effective in many applications. Mainly the efficiency of WSNs is depends of the correctness of the information that have been collected by the sensors. In many critical applications it is necessary to protect the sensor network from malicious attacks which demands providing security mechanisms in the network. The major challenge for implementing an efficient security mechanism in WSN is the resource constrained nature of WSNs like sensor size, processing power memory, battery power, low bandwidth etc. The accessibility of wireless channel by the attackers is also a reasonable challenge for implementation of security.

Now a day a large set of research is going in the field of security aspects of WSNs. Many of these are done by considering the layered approach of security, but exploring the security by considering the layered and cross layered communication is much more better .The cross layered design allows direct communication between protocols at non adjacent layers ie., they use the same variables at different layers for communication

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

## II. LITERATURE REVIEW

The security of wireless sensor networks is an area that has been discussed extremely through a few years ago. Networks have different applications and these applications comprise several levels of monitoring, tracking, and controlling. Wireless sensor networks consist of enormous number of small nodes. These nodes are deployed in some important areas. These nodes sense the data then integrate these data and forward it to the base station for further processing. The security requirements of WSNs include data confidentiality, data integrity, data freshness, authentication, self organization of nodes, time synchronization, availability etc.

**Layered and cross layered security design approach in wireless sensor network [4-5]**

The recent researches shown that the layered model is not appropriate for WSNs. So the researchers have made some modification to the protocols which violate the layered approach (OSI Model). In OSI model the layered architecture defines a stack of protocol layers. Here each layer functions within a well defined boundary and perform some well defined functionalities. For implementing a change it is necessary to change the overall system architecture. Layered approach provides modularity, transparency, and standardization in the wired network. But this approach is not suited for WSNs. So we are looking for cross layered communication for enhancing the performance of sensor node. Cross layer design breaks the hierarchical layers of OSI model by merging of layers, implementation of new interfaces and provides additional inter dependencies between any two layers etc. It allows the communication between non adjacent layers of the protocols and sharing of variables between layers. It enables the interaction between different non adjacent layers and exchanging information between layers. The main benefits of cross layer designs include improvement in system performance increased network efficiency and the QOS for different applications .Cross layered design also provide energy efficiency and scalability. This cross layer design is sufficient for both wired and wireless networks.

**Security Schemes in Wireless Sensor Networks [6-8]**

For secure transmission of various types of information over networks, several cryptographic, stegnographic and other techniques are used. Here we discuss about various network security fundamentals and how all these techniques are meant for wireless sensor network.

**Authentication:** It is the process of determining whether someone or something is, in fact, who or what it declares itself to be. Authentication is the mechanism which provides access control to the users by checking the user's credentials with the credentials in a database of authorized users or in a data authentication server. Authentication enables organizations to keep their networks secure by permitting only authenticated users to access its protected resources, like computer systems, networks, databases, websites and other network-based applications or services. Authentication mechanisms are used to detect maliciously or spoofed packets. They are especially important in WSNs which use a shared wireless medium.

**Authorization:** Data authorization specifies access rights to resources and is strongly related to access control. Access control should prevent unauthorized users from participating in network resources. Hence, only authorized users can join a given network. Access control relies on access policies that are formalized, like access control rules in a computer system. Most modern operating systems include access control.

**Integrity:** Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data integrity is the quality of correctness, completeness, wholeness, soundness and compliance with the intention of the creators of the data. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people. Integrity ensures that data is real, accurate and safeguarded from unauthorized user. Modification is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people. In WSNs data integrity guarantees that a message being transferred is never corrupted, but providing data integrity is not

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

enough for wireless communication. The compromised sensor nodes can listen to transmitted messages and replay attacks.

**Confidentiality:** Confidentiality is roughly equivalent to privacy. A sensor node must not reveal the sensed data its neighbors even though it is routed through many nodes. Here we use different encryption mechanism to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. In WSN keeping sensitive data secret is the most important issue in case of critical applications in which highly sensitive data (secret keys, sensitive measurements, etc.) are collected and transmitted. Hence, measurement data should not be available to neighboring nodes, and secure channels between nodes should be created. To protect a network against cyber attacks and malicious nodes, the routing information and sensor identities should remain confidential too.

**Non-repudiation:** Non-repudiation is the assurance that someone cannot deny something. Typically, non repudiation refers to the ability to ensure that a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

**Privacy:** means that information is intelligible only to its rightful recipients. Although third parties may be able to read (a copy of) the message sent, they must not be able to make sense of it.

**Availability:** In secure network data should be safe and accessible at all times. Availability guarantees the survivability of network services against Denial-of-Service (DoS) attacks that can be launched at any layer of a wireless sensor network. It guarantees that the network services and resources are feasible even in the subsistence of denial of service attack

**Data freshness:** Data freshness protects data against replay attacks by ensuring that the transmitted data is recent one. It also ensures that no previous messages have been replayed by an adversary.

## Security Attacks in Wireless Sensor Networks

Attacks against wireless sensor networks could be broadly considered from two different levels of views. They are the attack against the security mechanisms and attacks against the routing mechanisms.

### Security Attacks on Sensor Network Routing

### Black hole

Black hole [9-11] is a kind of DOS attack which is very difficult to detect and defend. To send data from source to destination the source node starts the route discovering process by broadcasting route request to all its neighbors. All the neighbors receive the request and forward them to the destination by adding their address with it. A malicious node send the reply packet with highest sequence number and lowest hop count ,ie, Here a malicious node announces itself as the shortest path (or) the source node falsely identified it as the destination and this malicious node attract all the traffic in the sensor network towards itself. So the sender node transfers all the data packets to the adversary node. The node which acts as a black hole captures and reprograms a set of nodes in the networks to block the packets they received instead of forwarding them towards the base station. This causes high end to end delay and low throughput.

### Selective forwarding

Selective Forwarding:[12-13] In a selective forwarding attack an attacker nodes behaves like black hole and tries to prevent certain messages to reach at the neighboring nodes, instead simply drop them, ensuring that they are not propagated any further. But here neighboring nodes will conclude that they failed to receive the message and decide to

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

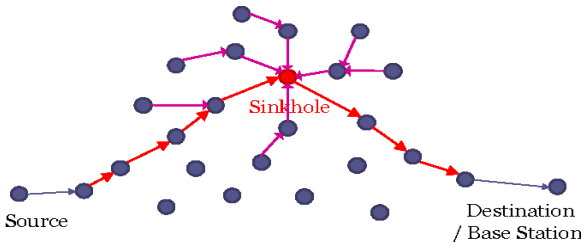
Vol. 8, Issue 5, May 2019

seek another route. An adversary who is interested in suppressing or modifying the packets originating from a few selected nodes can reliably forward the remaining traffic and limit feeling of this unlawful activity.

In selective forwarding attack the malicious node can selectively drops the packets coming from a particular node or a group of nodes. This behavior causes a DoS attack for that particular node or a group of node. (Or), the subverted node arbitrarily neglecting to route some messages this type of selective forwarding attack is called Neglect and Greed

**Sinkhole Attack**

Sinkhole attack [14-16] is basically a dangerous insider attack where the intruder compromises a node in the network and launches an attack. Sinkhole attacks are a type of network layer attack where the compromised node sends fake routing information to its neighbors to attract network traffic to itself. It can disrupt the network by modifying the routing packets. Sinkhole attack prevent the base station to gain all the correct sensing data and the attacker attract the network by adverting itself as the shortest path or high quality route to the base station .The attacker node receives the information and prevent the arrival of the information to the base station. This attack do not target to all the nodes in the network, instead it aims to only those nodes which are very close to the base station. The attacker node tries to create a high quality shortest single hop connection with the base station and then makes an advertisement with its features to all of its neighboring nodes. Thus the neighboring nodes routes their traffic to this intruder node. The goal of a sinkhole attack is to lure traffic to a malicious part of the network. Sensor networks are susceptible to these attacks due to their multihop nature and the specialized communication patterns they use.




Sinkhole attack

**Sybil Attack**

Wireless sensor network is vulnerable to the Sybil attack [17-18]. The Sybil attack targets fault tolerant schemes such as distributed storage, disparity, multipart routing and topology maintenance In this case a node /a malicious device claim multiple identities and may be able to acquire a disproportionate level of control over the network. These malicious multiple identities are referred as Sybil nodes and by outsiders these fake identity appear to be unique user. This type of attack tries to degrade the security, resource utilization and integrity of the data. To prevent Sybil attack various authentication and encryption mechanisms were used.

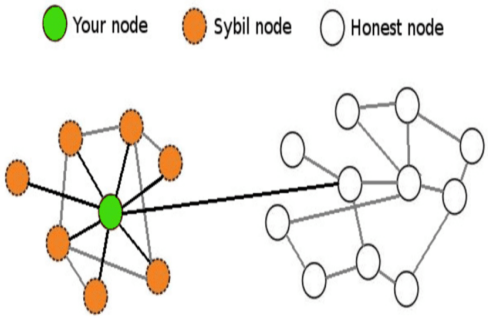
ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Visit: www.ijirset.com*

**Vol. 8, Issue 5, May 2019**

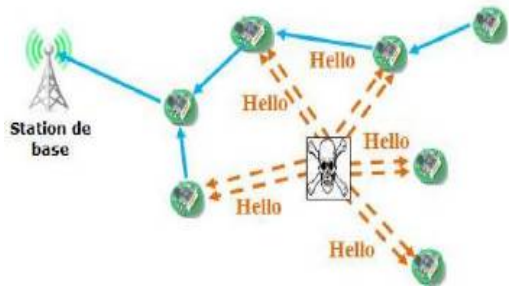



Sybil Attack

Here the multiple identities of the Sybil node is shown with orange coloured nodes it degrade the security of the network.

**Hello Flood Attack**

Hello flood [19] is the main attack in the network layer. In many protocols sometimes it is required for node to transmit HELLO packets to advertise itself to its neighboring nodes. The nodes receiving these packets assume that it is within the range of the sender. In HELLO flood attack a malicious node can send record or replay HELLO message with high transmission power. It creates an illusion of being a neighbor to many nodes in the network and may confuse the network badly. The size of these packets is very small and transmitted without any acknowledgement. Thus a large number of nodes in the network choose it as the base station and the messages are routed to this malicious node this causes the wastage of the energy




. Hello flood attack

Here the attacker with a high radio transmission range and processing power sends HELLO packet to a number of sensor nodes that they are separated in a large area within a wireless sensor network. Attacker with power to begin track broadcast, so that in the network each node is believed that attacker node is its neighbour and will send data to it.

**Spoofed, Altered or Replayed Routing Information** [20]

An unprotected ad hoc routing is vulnerable to these types of attacks here every node may act as a router and may therefore directly affect the routing information. a spoofing attack is a situation in which a person or program successfully masquerades as another by falsifying data, to gain an illegitimate advantage. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

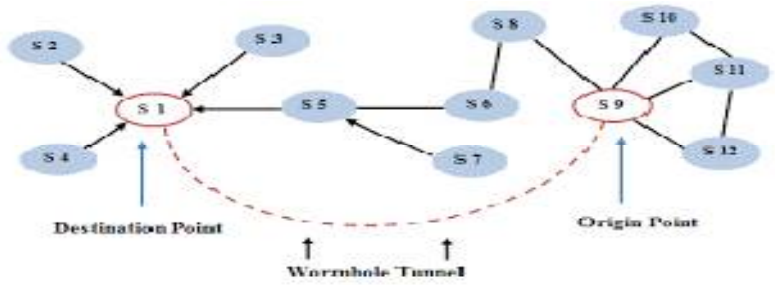
either by the originator or by an adversary who intercepts the data and re-transmits it, possibly as part of a masquerade attack by IP packet substitution. This is one of the lower tier versions of a "Man-in-the-middle attack". In a message modification (altered) attack, an intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine."

**Acknowledgment Spoofing**

In spoofing attack a person or program successfully masquerades as another by fabricating false data to gain an illegal advantage. Routing algorithms used in the sensor network environment are mostly based on acknowledgement. The protocols uses link layer acknowledgement for next hope based on reliability issues are susceptible to acknowledgement spoofing. Thus the attacker may spoof the acknowledgement and convincing the sender that a weak link may be strong or an inactive node is still alive. This causes an attacker to lure its neighbor to transmit the packet through a weak link and there for there is a high probability to lost the data packet or corruption of data.

**Wormholes**

A wormhole [21] is a tunnel (or) low latency link to another part of the network which is created by a malicious node. This malicious node talks into its neighbours itself as the shortest path to the base station and chooses it as the next hop. This malicious node may receive the packets from one part of the network and forward/ replayed the message to other session of the network. It will create congestion by misguiding the traffic into a single direction. It also creates the retransmission of data. This attack occurs at the network layer of WSN and very difficult to defend when it is combined with selective forwarding and Sybil attack.




Wormhole attack

Node S1 and node S9 are connected through a tunnel, ie, the shortest route provided by the wormhole to send data. Data will be caught by the malicious nodes and then by the attacker

**Attacks on Specific Sensor Network Protocols**

**TinyOS Beaconing**

The TinyOS beaconing protocol create a breadth first spanning tree rooted at a base station. It periodically broadcast the routing updates. On the reception of this updates the corresponding nodes mark the base station as its parent and then rebroadcast the update. The algorithm continues recursively with each node marking its parent as the first node from which it hears a routing update during the current time period. All packets received or generated by a node are

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

forwarded to its parent until they reach the base station. Security services provided by TinyOS beaconing protocol are integrity, Authentication, confidentiality replay protection etc.

Possible attacks: Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods

**Directed Diffusion**

Directed diffusion [22] has some novel features like data-centric dissemination, reinforcement based adaptation to the empirically best path, and in-network data aggregation and caching. These features can enable highly energy-efficient and robust dissemination in dynamic sensor networks. Directed diffusion consists of several elements. Data is **named** using attribute-value pairs. A sensing task (or a subtask thereof) is disseminated throughout the sensor network as an **interest** for named data. This dissemination sets up **gradients** within the network designed to "draw" events (i.e., data matching the interest). Events start flowing towards the originators of interests along multiple paths. The sensor network reinforces one, or a small number of these paths. Communication in directed diffusion is data-centric: interests, which specify events that are to be recorded, are propagated by sink nodes throughout the network via flooding. These initial requests for information stipulate that responses should be sent at a low data rate. Upon receiving responses from multiple sources, a sink can use positive and negative reinforcement to increase and decrease gradients' (i.e. paths') data rates, respectively. Reinforcement mechanisms can vary. Rules governing the propagation of control messages are executed locally—that is, each node decides individually, without global state, the policies determining how it will react to control messages.

Possible attacks: Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods

**Geographic Routing**

**Greedy Perimeter Stateless Routing (GPSR) [25]**

It is a routing protocol for wireless datagram networks. GPSR uses the positions of routers and a packet's destination to make packet forwarding decisions. GPSR makes greedy forwarding decisions using only information about a router's immediate neighbors in the network topology. When a packet reaches a region where greedy forwarding is impossible, the algorithm recovers by routing around the perimeter of the region. By keeping state only about the local topology, GPSR scales better in per-router state than shortest-path and ad-hoc routing protocols as the number of network destinations increases. Under mobility's frequent topology changes, GPSR can use local topology information to find correct new routes quickly. One drawback of GPSR is that packets along a single flow will always use the same nodes for the routing of each packet, leading to uneven energy consumption

**Geographic and Energy Aware Routing (GEAR)**[23]

This protocol uses energy aware and geographically informed neighbor selection to route a packet towards the target region and Recursive Geographic Forwarding or Restricted Flooding algorithm is used to disseminate the packet inside the destination region. This strategy attempts to balance energy consumption and thereby increase network lifetime than non-energy aware geographic routing algorithms. One drawback of GPSR is that packets along a single flow will always use the same nodes for the routing of each packet, leading to uneven energy consumption. GEAR attempts to remedy this problem by weighting the choice of the next hop by both remaining energy and distance from the target.

Possible attacks: Bogus routing information, selective forwarding, sinkholes, wormholes, HELLO floods

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

**LEACH**

LEACH (Low Energy Adaptive Clustering Hierarchy) [26-27] is a hierarchical protocol which is defined to reduce energy consumption by aggregating and compressing the data to reduce the transmission to the base station. It uses cluster based routing in order to minimize the energy consumption. The ultimate aim of the LEACH algorithm is to improve the life span of sensor nodes by choosing the appropriate cluster head. LEACH performs its operation in two phases. In first phase which is called setup phase it select the cluster head for each cluster of nodes with minimum energy .in this phase it performs 3 operations ie, cluster head advertisement, cluster setup, and creation of transmission schedule. In second phase each cluster head create the transmission schedule for the members of their cluster. It uses THMA scheduling where each node transmits its data in the allotted time slot. So it is called a TDMA based MAC protocol.

Possible attacks: Sybil stack Selective forwarding, HELLO floods

**Rumor Routing**

Rumor routing [28] is a logical compromise between query flooding and event flooding. It is a probabilistic protocol for matching queries with data events. Rumor routing offers an energy-efficient alternative when the high cost of flooding cannot be justified. Rumor routing is based on the concept of agent, which is a long-lived packet that traverses a network and informs each node it encounters about the events that it has learned during its network traverse. In rumor routing, when a source observes an event, it sends an agent on a random walk throughout the network. Agents carry a list of events, the next hop of paths to those events, the corresponding hop counts of those paths, a time to live (TTL) field, and a list of previously visited nodes and those nodes' neighbors (used to help "straighten" paths and eliminate loops). When an agent arrives at a new node, it informs that node of events it knows of (and the next hop on the path to those events), adds to its event list any events the node might know of, and decrements it's TTL. If the TTL is greater than zero, the node probabilistically chooses the agent's next hop from its own neighbors minus the previously seen nodes listed in the agent. When a base station wants to disseminate a query, it creates an agent that propagates in a similar way. A route from a base station to a source is established when a query agent arrives at a node previously traversed by an event agent that satisfies the query.

Possible attacks: Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes

**SPAN & GAF**

SPAN & GAF are location-based protocols. Here, sensor nodes are addressed by means of their locations. Location information for sensor nodes is mandatory for sensor networks by most of the routing protocols to compute the distance among two particular nodes so that energy consumption can be estimated.

GAF **(Geographic Adaptive Fidelity)[29** is an energy-aware routing protocol principally proposed for MANETs. It can also be used for WSNs because it favors energy conservation. It considers the energy conception during transmission and reception of packets. GAF also consider the idle time of the sensors when they do not detect the signal. GAF uses a mechanism of turning off unnecessary sensors while keeping a stable level of routing fidelity. In GAF the sensor field is divided into grid squares. Each and every sensor uses the location information to identify the other grid associated with it. The sensors or node belonging to the adjacent grid squares are able to communicate. The nodes are either in sleep mode, recovery mode or in active mode.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019


State diagram

In the active state, a sensor periodically broadcasts its discovery message to inform equivalent sensors about its state. They participate in routing. In sleeping mode the inactive node turns of its radio in order to save the energy. . In the discovery state, a node exchanges discovery messages to learn about other sensors in the same grid. Discovery messages are used to exchange state and ranking information between nodes in the same grid. The ranking of sensors is based on their residual energy levels ie, node with a higher rank will be able to handle routing within their corresponding grids. . GAF tries to maximize the network lifetime to reach a state in which each grid square has only one active sensor node.

Possible attacks: Bogus routing information, Sybil, HELLO floods

**SPAN**

The main goal of SPAN is to reduce the energy consumption of nodes. It also works on power conservation without compromising the capacity or connectivity of the nodes. Here a node is selected as the coordinator node among the nodes in the network participated in routing. There for it act as a backbone network. SPAN's election rule is required by each sensor to advertise its status as a coordinator or non coordinator. It uses the local information to elect the coordinator on the basis of radio range. Coordinators stay continuously in on state where as the remaining nodes goes to sleep mode. To avoid congestion the capacity and the backbone network formed with coordinators must be equal to the total capacity of the original network. Here load balancing is achieved by rotating the role of coordinators among all the nodes in the network. SPAN does not require sensors to know their location information. It runs well with geographic protocol. Here the coordinator forwards the packet on behalf of another sensor between source and destination. When a coordinator receives a packet it forwards the packet to a neighboring coordinator which is closest to the destination or to a non coordinator that is closer to the destination.

Possible attacks: Bogus routing information, Sybil, HELLO floods

## III. CONCLUSION

A wireless sensor network is a promising communication aspect for many applications. In this paper we present a general view of layered and cross layered design approach where cross layered design approach is suitable for overcoming some of the current limitations of layered protocol. Also this paper gives an idea about various security schemes, security attacks on specific sensor protocols and attacks on network routing

## REFERENCES

[1] A. Bagula, "Applications of wireless sensor networks", http://wireless.ictp.it/wp-content/uploads/2012/02 /WSN-Applications.pdf
[2] V. Potdar, A. Sharif, E. Chang, "Wireless sensor networks: a survey", In Proceedings of the International Conference on Advanced Information Networking and Applications Workshops, pp.636–641, 2009.
[3] J. Yick, B. Mukherjee, D. Ghosal, "Wireless sensor network survey,Computer Networks",The International Journal of Computer and Telecommunications Networking, Vol. 52, No 12. 2008, pp. 2292-2330.
[4] Rakesh Kumar Saini ,Ritika , Sandip Vijay "A Survey on Cross Layer Design implementation in Wireless Sensor Network" International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682 Vol.5, No.7, July 2016 pp. 101-107

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

*Visit: www.ijirset.com*

**Vol. 8, Issue 5, May 2019**

[5] Kalpana Sharma, M K Gose ,"Cross Layer Security Frame Work for Wireless sensor Network", International journal of security and application Vol 5 No.1 Jan 2011
[6] V. C. Giruka, M. Singhal, J. Royalty, and S. Varanasi, "Security in wireless sensor networks: Research article," Wireless Communications and Mobile Computing, vol. 8, no. 1, pp. 1–24, 2008.
[7] A. Singla and R. Sachdeva, "Review on security issues and attacks in wireless sensor networks," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 4, pp. 529–534, 2013.
[8] J. M. Kizza, "Guide to computer network security", 3rd ed. Springer, 2015.
[9] Zoran S.Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, "Security Issues in Wireless Sensor Networks", International Journal Of Communication, Issue 1, 106-115 Volume 2, 2008
[10] Sheela.D, Srividhya.V.R, Asma Begam, Anjali and Chidanand G.M. "Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent" International Conference on Artificial Intelligence and Embedded Systems (ICAIES'2012) July 15-16, 2012 Singapore
[11] Yawar Abbas Bangash, Qamar ud Din Abid, Alshreef Abed Ali A, Yahya E. A. Al-Salhi "Security Issues and Challenges in Wireless Sensor Networks: A Survey" IAENG International Journal of Computer Science, 44:2, IJCS_44_2_02 2017
[12] Jiang changyong, Zhang jianming. "The selective forwarding attacks detection in WSNs". Computer Engineering, 2009, 35(21):pp 140-143
[13] Wazir Zada Khan et.al "Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks"in I.J. Computer Network and Information Security, 2011, 1, 1-10.
[14] Sharma K. and Ghose M.K. "Wireless sensor networks: An overview on its security threats." IJCA, Mobile Ad-hoc Networks, 42-45. (2010).
[15] Krontiris,I., Dimitriou,T., Giannetsos,T. and Mpasoukos, M., "Intrusion Detection Sinkhole Attacks in Wireless Sensor Network. In Networking and Communications" 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing, (pp. 526-531). IEEE.
[16.] Edith C. H. Ngai, Jiangchuan Liu and Michael R. Lyu; "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks" IEEE International Conference on Communications, 2006, Volume 8, pp. 3383- 3389.
[17] Karen Hsu, Man-Kit Leung and Brian Su, "Security Analysis on Defenses against Sybil Attacks in Wireless Sensor Networks", Issue 2008(IEEE).
[18] R. Amuthavalli, Dr. R. S. Bhuvaneswaran, "Detection and Prevention of Sybil Attack In Wireless Sensor Network Employing Random Password Comparison Method ",Journal of Theoretical and Applied Information Technology Issue September 2014,Vol 67 No 1,236-246.
[19] Virendra Pal Singh; Sweta Jain; Jyoti Singhai," Hello Flood Attack and its Countermeasures in Wireless Sensor Networks", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010, 23-27
[20] Sachin LalarÀ, "Security in Wireless Sensor Networks: Issues and Security Mechanisms", International Journal of Current Engineering and Technology ,February 2014, Vol.4, No.1.
[21] Shree Raj, Khan R. A." Wormhole Attack in Wireless Sensor Network" International Journal of Computer Networks and Communications Security Vol.2, No.1, pp. 22–26,January 2014.
[22] Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin, John Heidemann, and Fabio SilvaDirected Diffusion:" A Scalable and Robust Communication Paradigm for Sensor Networks", In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCOM '00), August 2000, Boston, Massachussetts.
[23] Yan Yu, Ramesh Govindan, Deborah Estrin "Geographical and Energy Aware Routing: a recursive data dissemination protocol for wireless sensor networks"
[24] Chris Karlof David Wagner,"Secure Routing in Wireless Sensor Networks:Attacks and Countermeasures" Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003/ May
[25] Karp, B. and Kung, H.T., GPSR: "Greedy Perimeter Stateless Routing for Wireless Networks", in Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2000), Boston, MA, August, 2000, pages 243-254
[26] Reenkamal Kaur Gill, Priya Chawla and Monika Sachdeva,"Study of LEACH Routing Protocol for Wireless Sensor Networks" International Conference on Communication, Computing & Systems (ICCCS–2014)
[27] Rajesh Patel, Sunil Pariyani, Vijay Ukani," Energy and hroughput Analysis of Hierarchical Routing Protocol(LEACH) for Wireless Sensor Networks", International Journal of Computer Applications Volume 20- No. 4 (April 2011).
[28] D. Braginsky and D. Estrin. "Rumor routing algorthim for sensor networks." In WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, pages 22–31. ACM Press,2002.
[29] Hanane AZNAOUI, Said RAGHAY, and Layla AZIZ.,"Location-Based Routing Protocols GAF and its enhanced versions in Wireless Sensor Network a Survey " IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.6, June 2016,pages 151-156
[30] Harneet Kour," Hierarchical Routing Protocols In Wireless Sensor Networks", International Journal of Information Technology and Knowledge Management December 2012, Volume 6, No. 1. PP 47-52