A STUDY OF ROUTING PROTOCOLS AND SECURITY THREATS IN WIRELESS SENSOR NETWORK

Manjinder Kaur
Department of Electronics & Communication
Regional Campus, Guru Nanak Dev University
Gurdaspur, Punjab, India
manjinder.kaur424@gmail.com

Dr. Shashi B. Rana*
Department of Electronics & Communication
Regional Campus, Guru Nanak Dev University
Gurdaspur, Punjab, India
shashi_rana12@yahoo.co.in

Abstract-- Wireless Sensor Network is an emerging technology which is made up of a large number of sensor nodes, which are highly distributed with sensing, computation and wireless communication capability. Due to the broadcast nature in WSN there is a need of security. So as to assist applications which need data delivery derived from one or multiple senders to one or multiple receivers must need proper security mechanism. In this paper, we present different routing protocols used in WSN and various types of security issues in WSN.

Keywords- WSN, challenges, routing protocols, attacks.

I. INTRODUCTION

With the recent technological advances in wireless communications, processor, memory, radio, low power, highly integrated digital electronics, and micro electro mechanical systems (MEMS) [1]; it becomes possible to significantly develop tiny and small size, low power, and low priced multifunctional sensor nodes. These nodes are designed for wireless communications, sensing and computation (software, hardware, algorithms). So, it is clear that wireless sensor network is the consequence of the mixture of sensory techniques, embedded techniques, distributed information processing, and communication mechanisms. A wireless sensor network (WSN) [2] is a network that's made of hundreds or tens and thousands of the sensor nodes, that are heavily distributed in an unattended environment with the abilities of sensing, wireless communications and computations (i.e., collecting and broadcasting environmental data). Numerous routing, power management and data dissemination protocols have now been created for wireless sensor networks, influenced by both architectures of wireless sensor network and the applications that WSN is supposed to support. The WSN is created by few as well as a large number of sensor nodes, where each node is connected to one or sometimes several sensors. Each sensor network node has typically several parts: a radio transceiver by having an internal antenna or link with an additional antenna, a microcontroller, an electric circuit for interfacing with the sensors and a power source (i.e. battery or an embedded kind of energy harvesting). The topology of the WSNs, from a straight forward star network to an enhanced multi-hop wireless mesh network can vary. The propagation technique involving the hops of the network could be routing or flooding. A wireless sensor network is composed of three components: Sensors Nodes, Task Manager Node (User) and Interconnect Backbone, as shown in Figure 1.

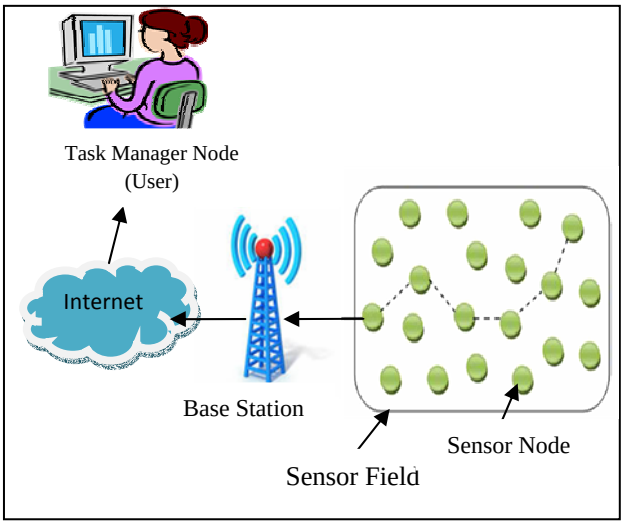

Figure 1: Wireless Sensor Network architecture

Each Sensor Node can contain various sensors and actuators that are accustomed to collect the information and control physical processes. The collected data is used in the User through the network that could include Internet segments. Besides collecting the original information and controlling actuators, a node might need to perform some computation on the measured data. Direct communication among individual nodes can be required. The Task Manager Node (User) performs tasks in data storage, analysis and display.

WSN Requirements: It must support the following requirements in deployment: reliability, scalability, responsiveness, mobility, and power efficiency. The description of those:

Reliability- It is the power of the network for reliable data transmission in circumstances of a continuous change of the network structure.

Scalability- It is the power of a network to deal with an increasing level of work in an able manner or its capability to be enlarged to allow for that growth.

Responsiveness- The power of the network to quickly adapt itself to changes in topology.

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

Challenges of WSN

The important challenges faced by WSNs are:

- Less power consumption
- Ability to cope with node failures
- Usability in large scale
- Survival in adverse environmental conditions
- Communication failures
- Heterogeneity of nodes

The rest of the paper is organized as follows: Section II reviews the related literature survey. The various routing protocols for WSN are discussed in Section III. Section IV describes various security issues in WSN. Finally Section V concludes the paper.

II. LITERATURE SURVEY

K. Sohrabi, et al.[2](2000) present their state of the art of wireless sensor networks' architecture and design features. They also introduce recent work with routing protocols for WSNs and their design goals and challenges. In their paper, several open research questions of wireless sensor networks management and issues are suggested and put forward. I. Akyildiz *et al.* [3](2002) presented a thorough overview of the recent literature on various areas of WSNs and discuss how a wireless sensor network works and the advantages and disadvantages within the traditional network. Wendi B. Heinzelman *et al.* [4](2002) developed and analyzed low-energy adaptive clustering hierarchy (LEACH), a protocol architecture for sensor networks that combines the ideas of energy-efficient cluster-based routing and media access together with application-specific data aggregation to achieve good performance in terms of system lifetime, latency, and application-perceived quality. C. Karlof *et al*. [5](2003) was the first one to describe the various the vulnerabilities in WSN. They propose security goals for routing in sensor networks, present general classes of attacks, and analyze the security of the majority of the currently documented sensor network routing protocols and energy conserving topology maintenance algorithms. Parul Tyagi *et al*. [6](2012) analyze recent routing protocols for wireless sensor network and classify in three forms of approaches in accordance with network architecture in WSN i.e. Flat, Hierarchical and location based routing protocols. They also study tradeoff between energy and communication overhead savings in each routing protocols as well as highlighted the advantages and performance issues of every routing technique. H.H. Soliman *et al.* [7](2012) evaluates and compares the most prominent anomaly-based Intrusion detection system (IDS) systems for hierarchical WSNs and identify their strengths and weaknesses. For every IDS, the architecture and the related functionality are briefly introduced, discussed, and compared, focusing on both operational strengths and weakness. Furthermore, a contrast of the studied IDSs is carried out using some critical evaluation metrics which are split into two groups; the initial one linked to performance and the next linked to security. Finally on the basis of the carried evaluation and comparison, some design principles are concluded, which need to be addressed and satisfied in future research of designing and implementing IDS for WSNs. Yusnani Mohd Yussoff *et al.* [8](2012) presents the review on physical attacks accompanied by the introduction of trusted platform with protected memory that not merely protect sensor node's sensitive credentials but provide a concrete method to trust nodes in the dedicated wireless sensor network. Also summarization of proposed IBE_Trust framework is presented and briefly discussed. Wen Tao Zhu *et al.* [9](2012) discuss a typical threat in the latter category referred to as the node replication attack, where an

adversary prepares her very own low-cost sensor nodes and deceives the network into accepting them as legitimate ones. To do this, the adversary only must physically capture one node, extract its secret credentials, reproduce the node in large quantity, and then deploy the replicas under her control into the network, possibly at strategic positions, to cripple various WSN applications with little effort. In addition they present the technical challenges and indicate some possible directions for future research. Aashima Singla *et al.* [10](2013) discussed concerning security in sensor networks, security issues and various DoS attacks on different layers. They also discuss various dimensions of security (availability, integrity, confidentiality and authenticity) that can be being directed by different physical attacks. Muhammad R. Ahmed *et al.* [11](2013) use Dempster-Shafer theory (DST) of combined multiple evidences to spot the malicious or internal attacks in a WSN. They also provide a numerical process of fusing together multiple items of evidences from an unreliable neighbor with higher levels of conflict reliability. Sudhanshu Tyagi *et al.* [12](2013) offer the taxonomy of varied clustering and routing techniques in WSNs based upon the standard LEACH protocol in relation to metrics such as for instance power management, energy management, network lifetime, optimal cluster head selection, multihop data transmission etc. They also highlighted the relative advantages and disadvantages of lots of the prominent proposals in this category which supports the designers to choose a certain proposal in relation to its merits within the others. Nitesh Gondwal *et al.* [13](2013) propose a technique to detect the black-hole attack using multiple base-stations and a check always agent based technology. Check agent is a computer software program which will be self-controlling and it moves from node to node and checks the clear presence of black-hole nodes in the network. Their technique is energy efficient, fast, lightweight and reduces message complexity. Meenakshi Tripathi *et al.* [14](2013) provides summary of LEACH, the most used clustered routing protocol of WSN and how LEACH may be compromised by Black hole and Gray Hole attacker. They make use of "High energy threshold" concept to simulate these attacks on NS-2. The performance of WSN under attack is thoroughly investigated, through the use of it on various network parameters with various node densities. They have also floated a concept for detection of the attacks. Sneha M. Sakharkar *et al.* [15](2014) tried to explore security issues in WSN. They make use of Ad-hoc On Demand Distance (AODV) Vector scheme for detecting Gray-Hole attack and Statistical En-Route Filtering is used for detecting false report. For increasing security level, the Elliptic Curve Cryptography (ECC) algorithm is used. Zhao Han *et al.* [16](2014) we propose a General Self-Organized Tree-Based Energy-Balance routing protocol (GSTEB) which builds a routing tree using a procedure where, for every round, BS assigns a root node and broadcasts this selection to any or all sensor nodes. Subsequently, each node selects its parent by considering only itself and its neighbors' information, thus making GSTEB a powerful protocol. They also show that GSTEB has a better performance than other protocols in balancing energy consumption, thus prolonging the duration of WSN and provides better security than any other existing routing protocol.

III. ROUTING PROTOCOLS IN WSN

In a wireless sensor network, sensor nodes are constrained to limited resources itself, so the key target is to create an effective and energy aware protocol to be able to improve the network lifetime for specific application environment. Since sensor nodes aren't given a unique ID for identification and much redundant data collected at destination nodes. So, energy efficiency, scalability, latency, fault-tolerance, accuracy and QOS are some aspects which must certainly be taken into account while designing the routing protocols in wireless sensor networks. Routing in WSN is different from conventional routing as this doesn't have infrastructure, wireless links are unpredictable, sensor nodes may stop working and routing protocols have to hook up strict economical requirements. Many routing algorithms were produced for wireless networks. All major routing protocols [2] classified into three main categories as shown in Figure 2.

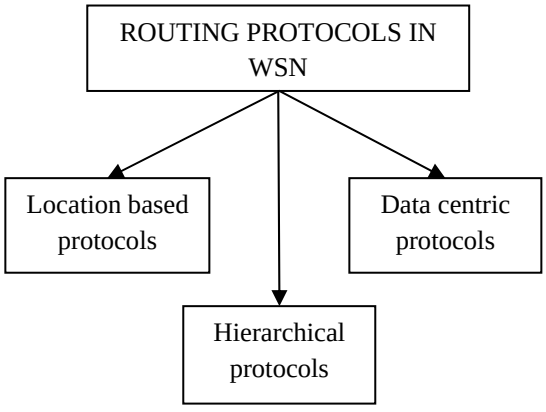

Figure 2: Classification of Routing protocols for Wireless Sensor Network

A. Location Based Protocols

The location information based routing protocol [6] uses location information to steer routing discovery and maintenance in addition to data forwarding, enabling directional transmission of the data and avoiding information flooding in the whole network. Location information is required to be able to calculate the exact distance between two particular nodes in order that energy consumption may be estimated. All major location based routing protocols are given in Figure 3.

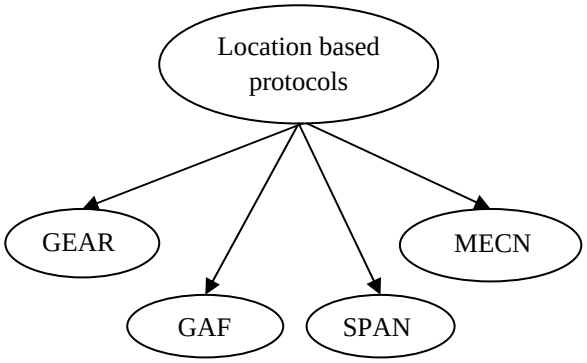

Figure 3: Classification of Location based protocols

Important location based protocols are:

i. GEAR

In this algorithm, each node keeps an estimated cost and an understanding cost of achieving the destination through neighbors. The estimated cost is a variety of residual energy and distance to destination. A hole occurs each time a node does have no closer neighbors to the target. If you can find no holes, the estimated cost adds up to the land cost. The land cost is propagated one hop back each time a packet reaches the destination to ensure that route create for next packet is likely to be adjusted.

ii. Geographic Adaptive Fidelity (GAF)

GAF is useful for WSN as it favors energy conversation. As shown in Figure 4, their state transition diagram has three stages, discovery, active and sleeping. When a sensor enters the sleeping state, it turns off radio for power saving. In discovery state, sensor exchange discovery messages to master about other sensors in the grid. In active state, sensor periodically broadcast its discovery message to see equivalent sensors about its state. GAF thus reduces the number of nodes required to make a network and saves battery power.

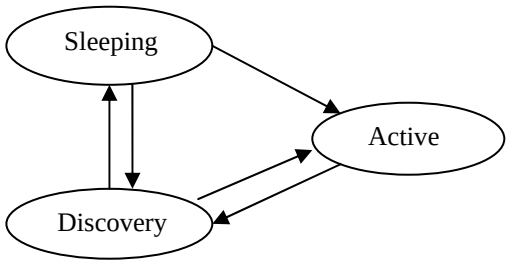

Figure 4: State Transition Diagram of GAF

B. Hierarchical Protocols

Clustering is a power efficient communication protocol that can be utilized by the sensors to report their sensed data to the sink. Hierarchical routing [17] is always to efficiently maintain the vitality use of the network. This allows inherent optimization capabilities at the cluster heads. A network consists of several clusters. Each cluster is managed with a special node, called cluster head that is accountable for coordinating the information transmission activities of sensors in its cluster. Representative Protocols of hierarchical routing are the following:

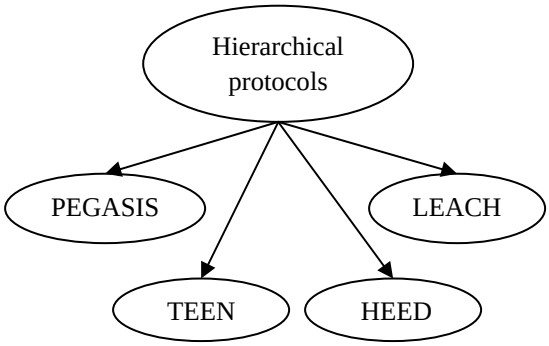

Figure 5: Classification of Hierarchical protocols

Let's have a look on widely used hierarchical protocols.

i. LEACH

Low energy adaptive clustering hierarchy (LEACH) [4] is a popular hierarchical routing protocol for sensor networks. LEACH is a hierarchical protocol where most nodes transmit to cluster heads, and the cluster heads compress and aggregate the information and forward it to the base station. LEACH assumes that every node features a radio powerful enough to directly reach the base station or the nearest cluster head, but by applying this radio at full power constantly would waste energy. Nodes which were cluster heads cannot become cluster heads again for P rounds. At the end of every round, each node that is not a

cluster head selects the closest cluster head and joins that cluster to transmit its data. LEACH centered on two basic assumptions:
(a) base station is fixed and located far from the sensors.
(b) all nodes in the network are homogeneous and energy constrained.

The concept behind LEACH is to make clusters of the sensor nodes with respect to the received signal strength and use local cluster heads as routers to route data to the base station. LEACH algorithm works as follows:

a) Advertisement phase: In this phase, nodes elect themselves to be always a cluster-heads for the present round I through a cluster-head advertisement message. With this cluster-head advertisement, the cluster heads use CSMA MAC protocol. Following the completion of the phase, and with respect to the received advertisement signal strength; the non cluster-head nodes (their receivers must certainly be maintained in this phase to hear the advertisements of most cluster-heads) determine the cluster to which they belong to for this current round I. At each round, a node n selects a random number k that's between 0 and 1. If k is less than the usual threshold T (n), then your node becomes a cluster-head for the present round I.

$$T(n) = \begin{cases} \dfrac{P}{1 - P\left(r \bmod \left(\frac{1}{P}\right)\right)}, & if\ n \in S \\ 0, & otherwise, \end{cases} \quad (1)$$

Where P is the desired percentage of cluster-heads, r is the current round, and S is the set of nodes that have not been cluster heads in the last $1/P$ rounds. Since k is randomly selected, then number of cluster heads may not be fixed.

b) Cluster set-up phase: After each non-cluster-head node will have chosen to which cluster it belongs, it informs the cluster-head node so it will be a member of the cluster. So, each node transmits these details back once again to the cluster head using CSMA MAC protocol.

c) Schedule Creation phase: The cluster-head node receives all the messages for nodes that wish to be contained in the cluster. Based on the quantity of nodes in the cluster, the cluster-head node makes a TDMA schedule telling each node if this can transmit. This schedule is broadcast back towards the nodes inside the cluster.

d) Data Transmission phase: After the creation of both the clusters and the TDMA schedule (TDMA is fixed), nodes in the cluster start transmitting the data they currently have throughout their allocated transmission time to the cluster-head (cluster-head node keeps its receiver on all the time to receive the sent data). Once all the data (sent by nodes in the cluster) have been received by the cluster-head node, it will perform signal processing function to compress the data into a single signal (the steady-state operation of LEACH networks).

Although, LEACH has shown good features to the sensor networks, such as for example, clustering architecture, localized coordination and control, randomized rotation of cluster head, and local compression to lessen global communications (energy consumption minimization), it suffers from the following drawbacks:
a) It can't be put on time-constrained application as it results in a long latency.
b) The nodes on the route a hotspot to the sink could drain their power fast. This issue referred to as "hotspot" problem.
c) How many clusters may not be fixed every round due to the selection of k.
d) It can't be put on large sensor networks.

ii. PEGASIS

PEGASIS (Power-Efficient Gathering in Sensor Information Systems) is a greedy chain-based power efficient algorithm [18]. Also, PEGASIS is dependent on LEACH (the scenario and the air model in PEGASIS are exactly like in LEACH). The important thing top features of PEGASIS are
a) The BS is fixed at a much distance from the sensor nodes.
b) The sensor nodes are homogeneous and energy constrained with uniform energy.
c) No mobility of sensor nodes.

PEGASIS is dependent on two ideas; Chaining, and Data Fusion. In PEGASIS, each node will take turn to be a leader of the chain, where in fact the chain could be constructed using greedy algorithms which are deployed by the sensor nodes. PEGASIS assumes that sensor nodes have an international understanding of the network, nodes are stationary (no movement of sensor nodes), and nodes have location details about all the nodes. PEGASIS performs data fusion accept the conclusion nodes in the chain. PEGASIS outperforms LEACH by reducing the

overhead of dynamic cluster formation, minimizing the amount of distances that non leader-nodes must transmit, limiting how many transmissions and receives among all nodes, and using only 1 transmission to the BS per round. PEGASIS has the same conditions that LEACH suffers from. Also, PEGASIS doesn't scale, can't be placed on sensor network where global understanding of the network is difficult to get.

iii. GSTEB

The key aim of General Self-Organized Tree-Based Energy-Balance Routing Protocol **(**GSTEB) [16] is to reach an extended network lifetime for different applications. In each round, BS assigns a root node and broadcasts its ID and its coordinates to all or any sensor nodes. Then your network computes the road either by transmitting the road information from BS to sensor nodes or with the same tree structure being dynamically and individually built by each node. For both cases, GSTEB may change the basis and reconstruct the routing tree with short delay and low energy consumption. The operation of GSTEB is divided in to Initial Phase, Tree Constructing Phase, Self-Organized Data Collecting and Transmitting Phase, and Information Exchanging Phase.

a) Initial Phase: When Initial Phase begins, base station broadcasts a packet to all or any the nodes to share with them of beginning time. Each node sends its packet in a group with a particular radius during a unique time slot. Each node sends a packet which contains all its neighbors' information during a unique time slot. Then its neighbors can receive this packet and record the info in memory. Initial Phase is just a significant preparation for other phases [14]. After Initial Phase, GSTEB operates in rounds. In a round, the routing tree may be rebuilt and each sensor node generates data packet that really needs to be provided for base station. When base station receives the information of most sensor nodes, a round finished

b) Tree Constructing Phase: BS assigns a node as root and broadcasts root ID and root coordinates to any or all sensor nodes. In each round, a node with the greatest residual energy is chosen as root. The root collects the data of most sensors and transmits the fused data to base station over long distance. Each node tries to choose a parent in its neighbors using vitality. The nodes will compute their energy level by using the function,

$$EL = \frac{Residual\ energy(i)}{\alpha} \quad (2)$$

In the equation 2, where '*i*' may be the ID of every node, and α is a constant which reflects the minimum energy unit and may be changed predicated on our demands. The length between parent node and the primary needs to be shorter than that between it and the root. Because every node selects the parent from its neighbors and every node records its neighbors' information in the table. Each node is fully aware of all its neighbors' parent nodes by computing, and additionally, it knows all its child nodes. In case a node does not have any child node, it defines itself as a leaf node from that data transmission begins.

c) Self-Organized Data Collecting and Transmitting Phase: Once the routing tree is constructed, each sensor node gathers information to develop a data packet which must be transmitted to base station. After having a node receives every piece of information from its child nodes, this node itself functions as a leaf node and tries to send the fused data in next time slot. The initial segment is required to examine if you have communication interference for a parent node. During this segment, each leaf node sends a beacon that contains its ID to its parent node at the same time. Each node chooses its parent by considering not the length but the entire energy consumption.

d) Information Exchanging Phase: Each node must generate and transmit a data packet in each round, before it drains its energy and dies. The dying of any sensor node can influence the topography .So the nodes that are likely to die need to share with other nodes .The process can also be split into time slots and in every time slot, the nodes whose energy will probably be exhausted will compute a random delay helping to make only 1 node broadcast in new slot. Once the delay is ended, these nodes will make an effort to broadcast a package to the complete network. While all the nodes are monitoring the channel, they'll receive this packet and perform an ID check. So, the cluster head is selected on the basis of the degree of energy in order that information may be transferred securely.

IV. SECURITY ISSUES IN WSN

Security is one of the main characteristic of any system. Wireless sensor networks are power restraint networks, having restricted computational as well as energy

resources. This makes them exposed enough to be attacked by any attacker deploying more resources than any individual node or base station, which might not be an arduous work for the attacker. A normal sensor network might be made up of potentially a huge collection of nodes which can use broadcast or multicast transmission. The broadcast nature of the transmission medium is the paramount reason wireless sensor networks are prone to security attacks.

These attacks can be categorized as:

1. Attacks on secrecy and authentication
2. Silent attacks on service integrity
3. Attacks on network availability

Attacks on network availability are also known as denial of service (DoS) attacks [19]. If DoS attacks are promoted effectively, it can badly degrade the performance of WSNs. Below we discuss the DoS attacks on different layers of networks:

DoS attacks on the physical layer: Physical layer is engaged with carrier frequency generation, frequency selection, signal detection, modulation and forward error correction. Jamming is the most frequent means of injecting DoS attack with this layer.

DoS attacks on the link layer: Data link layer is subjected to multiplexing of data streams, data frame detection, medium access control and error control. The attacks when elevated with this layer results in collision, resource exhaustion and unfairness in allocation of frames.

DoS attacks on the network layer: Network layer is subjected to various kinds of attacks such as for instance spoofed routing information, selective forwarding, sinkhole, sybil, wormhole and acknowledgment flooding.

DoS attacks on the transport layer: Transport layer is subjected to flooding attack and de-synchronization attack.

DoS attacks on the application layer: Application layer is subjected to logic errors and buffer overflow.

Different DoS attacks on different layers are:

A. Spoofed, altered, or replayed routing information
B. Selective forwarding
C. Jamming
D. Physical attacks
E. Sinkhole attacks
F. Sybil attacks
G. Wormholes
H. Black hole attacks
I. Gray hole attacks
J. Acknowledgement spoofing

A. Spoofed, altered, or replayed routing information

One of the most direct attacks against a routing protocol is to target the details exchanged between nodes. The attacker can probably create the routing loop, increase or decrease source path, generate false error messages, partition the network, and increases end to absolve delay. Most of these attacks generally occur at the physical layer. These attacks are generally possible on hierarchical based routing protocols.

B. Selective forwarding

Multi-hop networks tend to be on the basis of the assumption that participating nodes will faithfully forward messages received. In a selective forwarding attack, malicious nodes may not forward certain messages and simply drop them, ensuring that they do not propagated any further. A straight forward form of the attack is each time a malicious node behaves just like a black hole [13] and will not forward every packet it sees. This attack occurs at the network layer. Such an attack is possible on hierarchical based routing protocols, location based routing protocols, Network flow and QoS aware protocols. Selective forwarding attacks are generally more reliable once the attacker is explicitly included on the trail of a data flow. Figure 6 shows scenarios of selective forward its data forward attack where source node ‘S’ forwards its data packets D1, D2, D3 to node ‘A’ and ‘A’ forward these received packets to node ‘B’. On other hand an attacker node AD selectively forwards packets D1, D3 while dropping packet D2.

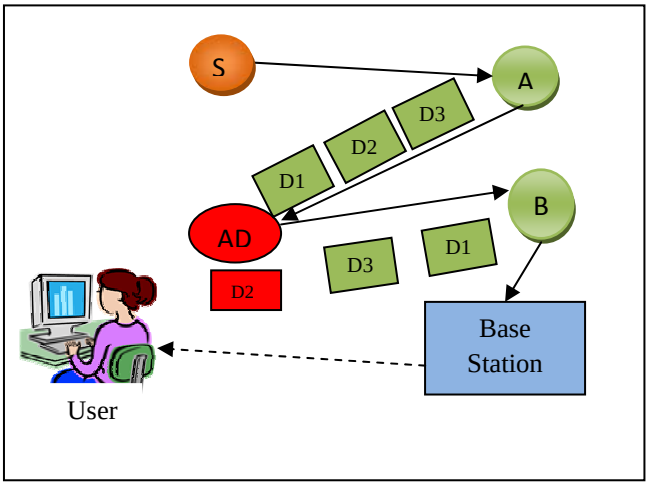

Figure 6: Selective Forward attack

C. Jamming

Jamming has been one of many basic yet destructive attacks that try to interrupt in the physical layer of the WSN structure. Jamming may be of two types- constant

jamming and intermittent jamming. Constant jamming affects the whole obstruct of the complete network whereas in intermittent jamming nodes are designed for communicating data periodically although not continuously.

D. Physical Attacks

Physical attacks [8] could be broadly considered attacks which entail direct physical access by adversary towards the sensor node. Usually after capturing the node, the adversary proceeds to alter the classified data before redeploying the node into the network. Therefore, the results of physical attack are unsafe because it can cause various data exposures along with various other attacks.

E. Sinkhole attacks

In a sinkhole attack, the attacker's aim is always to lure almost all the traffic from the particular area via a compromised node, making a symbolic sinkhole with the attacker at the center. The attacker targets a spot to produce sinkhole where it may lure the best traffic, possibly nearer to the base station in order that the attacker node may very well be regarded as a base station. Sinkhole attacks can enable a number of other attacks (selective forwarding, for example). This attack occurs at the network layer. Such type of attack occurs in flat based routing protocol, hierarchical routing protocols, Network flow and QoS aware routing protocols.

F. Sybil attack

As in WSN, the routing protocols suppose that every node in the network has a distinctive identity. Within the Sybil attack [20], the attacker, i.e. Sybil node tries to falsify multiple regions by creating fake identities of nodes located close to the communication range. Multiple identities are usually occupied inside the sensor network either by falsehood or stealing the identities of genuine nodes. Sybil attack is a threat to location based routing protocols. This attack occurs at the network layer. This sort of attack can be done on flat based routing protocols, hierarchical routing protocols, location based routing protocols.

G. Wormholes

In the wormhole attack [21], set of bad nodes firstly discovers a wormhole at the network layer. A wormhole is just a low-latency junction between two parts of a network. The malicious node receives packets in a single element of the network and sends them to some other element of the network. These packets are then replayed locally. This creates a phony scenario that the initial sender is a couple of nodes far from the remote location. This might cause congestion and retransmission of packets squandering the power of innocent nodes.

H. Black Hole Attack

In the black-hole attack [13], attacker node collects a large amount of data and after that drops it. The black hole attack places an attacker node in the range of base station and lures the entire traffic to pass through it by advertising itself as shortest path. Then the attacker node drops some packets of data from any particular source in the network. Here, these re-programmed nodes are termed as black hole nodes and the region containing the black-hole nodes are black hole region. This type of attack occurs at the physical layer. This attack is possible on flat based routing protocols, hierarchical protocols, location based routing protocols and Network flow and QoS aware routing protocols. In the figure 7, BH is the black hole which first convenes the network that it is the nearest node to base station and attracts the network to route data through it. When it receives data from neighboring nodes it drops them.

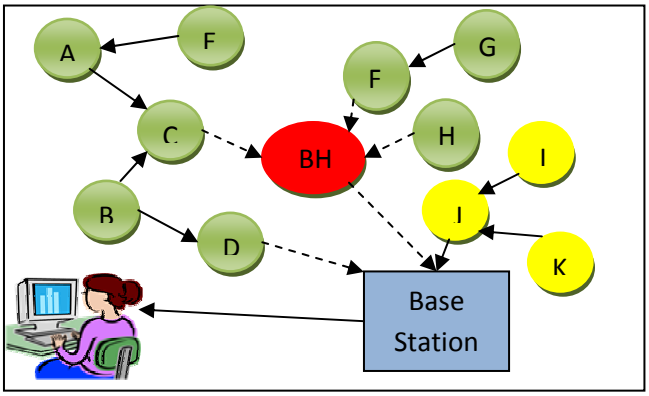

Figure 7: Black Hole attack

I. Gray Hole Attack

In Gray Hole attack [22], an attacker node reasonably refuses to send some packets thus drop them. A Gray Hole may exhibit its malicious behavior in multiple ways. It just drops all packets via certain specific node(s) in the network just like black hole attack. Another kind of Gray Hole attack is that where a node behaves maliciously for a few particular time duration by dropping packets, but may switch to normal behavior later A Gray Hole might also exhibit a random behavior like selective forwarding in which it drops a number of the packets arbitrarily while forwarding other packets, thereby making its detection much more difficult.

J. Acknowledgement spoofing

Routing algorithms utilized in wireless sensor networks sometimes require acknowledgements for being used. An attacking node can spoof the acknowledgements of overhead packets destined for neighboring nodes so as to afford false information to those neighboring nodes. An instance of such false facts is claiming a node is alive when it is dead. Artificiality reinforcing a poor or dead link is really a subtle means of manipulating this type of scheme. Since packets sent along with weak or dead links are lost, an attacker can effectively mount a selective forwarding attack using acknowledgement spoofing by encouraging the target node to transmit packets on those links.

TABLE 1 SUMMARY OF VARIOUS SECURITY ISSUES FOR WIRELESS SENSOR NETWORK

ATTACKS	LAYERS	PROTOCOLS
Spoofed, altered, or replayed routing information	Physical Layer	Hierarchical
Selective forwarding	Physical Layer	Hierarchical, location based, Network flow
Jamming	Physical Layer	Flat based, hierarchical, Network flow and QoS aware
Physical Attack	Physical Layer	Flat based, hierarchical, Network flow
Sinkhole Attack	Physical Layer	Flat based, hierarchical, Network flow and QoS aware
Sybil Attack	Network Layer	Flat based, hierarchical, location based
Wormholes	Network Layer	Flat based, hierarchical, location based, Network flow and QoS aware
Black Hole Attack	Network Layer	Flat based, hierarchical, location based, Network flow and QoS aware
Gray Hole Attack	Network Layer	Flat based, hierarchical, Network flow and QoS aware
Acknowledgement spoofing	Physical Layer	Hierarchical, location based, Network flow and QoS aware

V. CONCLUSION

In this paper, we present a brief overview of wireless sensor network, its characteristics and challenges. As the security in wireless sensor network has become an important issue. So we discussed security issues and various Dos attacks on different layers. Then different families of routing protocols are discussed among which no protocol was created yet to take good care of all security issues in WSN. Even many protocols are about to every security attack. Attacks like wormhole, sniffing, black hole and gray hole are possible on every routing protocol. In Table 1 various security issues are summarized for wireless sensor networks. This paper has not proposed any new mechanism to detect and control packets. So in near future we will propose a new secured tree based protocol to enhance the results further in wireless sensor network.

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] C. Karlof and D.Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Special Issue on Sensor Network Applications and Protocols vol. 1(2-3), pp. 1293 –1303, 2003.
[6] 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.
[7] H.H. Soliman, Noha A. Hikal and Nehal A. Sakr, "A comparative performance evaluation of intrusion detection techniques for hierarchical wireless sensor networks," Egyptian Informatics Journal vol. 13, pp. 225–238, 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] Wen Tao Zhu, Jianying Zhou, Robert H. Deng and Feng Bao, "Detecting node replication attacks in wireless sensor networks: A survey," Journal of Network and Computer Applications vol. 35 pp. 1022–1034, 2012.
[10] 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.
[11] Muhammad R. Ahmed, Xu Huang, and Hongyan Cui, "A Novel Evidential Evaluation for Internal Attacks with Dempster-Shafer Theory in WSN," 12th IEEE International Conference on Trust, Security and Privacy Computing and Communications (TrustCom), pp. 688-693. IEEE, 2013.
[12] Sudhanshu Tyagi and Neeraj Kumar, "A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks," Journal of Network and Computer Applications vol. 36, pp.623–645, 2013.
[13] 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.
[14] Meenakshi Tripathi, M.S. Gaur and V.Laxmi, "Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN", In 8th International Symposium on Intelligent Systems Techniques for Ad Hoc and Wireless Sensor Networks,vol.19, pp. 1101 – 1107, 2013.
[15] Sneha M. Sakharkar, R. S. Mangrulkar, and Mohammad Atique, "A survey: A secure routing method for detecting false reports and gray-hole attacks along with Elliptic Curve Cryptography in wireless sensor networks," In Electrical, Electronics and Computer Science (SCEECS), pp. 1-5, 2014.
[16] 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.
[17] 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, Issue 6, 2014.
[18] S. Lindsey, C. S. Raghavendra, "PEGASIS: Power- Efficient Gathering in Sensor Information Systems," presented at Proc. of IEEE Aerospace Conference, Montana, 2002.
[19] Jyoti Shukla, Babli Kumari, "Security Threats and Defense Approaches in Wireless Sensor Networks: An Overview," International Journal of Application or Innovation in Engineering & Management, vol. 2, Issue 3, March 2013
[20] J. R. Douceur, "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems, March 2002.
[21] 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.
[22] 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.
[23] K. Akkaya, and M. Younis, "A survey on Routing Protocols for Wireless Sensor Networks," Elsevier Ad Hoc network Journal, vol.3, pp.325-349, 2005.
[24]S. Upadhyayula, S.K.S. Gupta, "Spanning tree based algorithms for low latency and energy efficient data aggregation enhanced converge cast (DAC) in wireless sensor networks, Ad Hoc Networks, vol.5, pp.626–648, 2007.
[25] Andrei Gagarin, Sajid Hussain, Laurence T. Yang, "Distributed hierarchical search for balanced energy consumption routing spanning trees in wireless sensor networks," J. Parallel Distribution Computer, vol.70, pp.975-982, 2010.
[26] G.Asha, S.Durgadevi,Mr.K.Shankar, "The comparison between routing protocols based on lifetime of wireless sensor networks," International Journal of Engineering Science Invention, vol.3 Issue 11, pp.20-26, November 2014.
[27] Wenjing Guo, Wei Zhang, "A survey on intelligent routing protocols in wireless sensor networks," Journal of Network and Computer Applications, vol.38, pp.185–201, 2014.
[28] Shazana Md Zin, Nor BadrulAnuar, Miss Laiha Mat Kiah, Al-Sakib Khan Pathan, "Routing protocol design for secure WSN: Review and open research issues," Journal of Network and Computer Applications, vol.41, pp.517–530, 2014.

AUTHORS PROFILE

Manjinder Kaur has done her B.Tech in Electronics & Communication engineering from Punjab Technical University, India in year 2013. She is currently pursuing doing her MTech dissertation at Regional Campus (Gurdaspur), Guru Nanak Dev University, Punjab in Department of ECE with specialization in Communication Systems.

Dr. Shashi B. Rana, is currently working as an Associate Professor in the Department of Electronics & Communication Engineering at Regional campus (Gurdaspur), Guru Nanak Dev University, Punjab. He has published more than 25 research papers in International Referred Journals. His areas of interest are VLSI design and Nano Technology.