A Survey on Routing Techniques, Routing Attacks and Security Mechanisms in WSN

Ms. D. Sathya,
Assistant Professor II,
Department of Computer Science and Engineering,
Kumaraguru College of Technology,
Coimbatore, India,

ABSTRACT

Wireless Sensor Network (WSN) consists of large number of nodes and few base stations. These sensor nodes are spatially distributed to monitor physical or environmental conditions. The wireless sensor network existing in numerous application areas including military, industries, health monitoring, Area monitoring, Environmental sensing, Structural Monitoring etc. Today the security is a major issue in wireless sensor network. Since the attacks on sensor nodes may destruct the whole network and the sensitive information will be open to the intruders. The paper focuses mainly on the routing techniques, routing attacks, detection, prevention and avoidance of these attacks.

Keywords*: Wireless sensor network, routing types, routing attacks, defensive mechanisms.*

1. INTRODUCTION

The Wireless Sensor Network consists of large number of sensor nodes and a few base stations or sink nodes deployed in a field to monitor physical or environmental conditions and pass their collected information through a network to a main location (Base Station). The WSN is built from a few or several hundreds of nodes, where each node is connected to one or more sensors. Each sensor node comprises sensing, transmitter, mobilizer, position finding system and power units. A base station may be a fixed node or a mobile node. The sensor nodes communicate among each other or communicate directly to a base station. The route from sensor node to base station directly affects the network lifetime ie, short routes may yield decreased lifetime and long routes composed of many sensor nodes may increase the network delay.

The real time applications like military applications requires minimal network delay,whereas applications performing statistical computations may require maximized network lifetime. So a different routing techniques have to be followed for different types of applications. Wireless sensor network is weaker to security attacks since it broadcasts all the information on the network. Once the information is open to the intruders then it will create a mass damage to the network [7].
The security goals for sensor network are [2]:

- Data Confidentiality- the data should be accessible only to the authorized users.
- Data Integrity- ensures that data packets are not altered and the data packets received at destination is exactly the same transferred by the sender.
- Data Availability- the data should be available on the request of authorized users.
- Self Organization – After deployment, sensor nodes are required to self-organize themselves to form a network of their own. Only the authorized nodes should be allowed to join the network.
- Data Freshness –the data should be recent and ensure no old packets have been replayed ie. measured in terms of latency or delay of packets received at the sink node.
- Time Synchronization- Group synchronization is required for tracking applications.
- Secure Localization – determining the location of a sensor is required for geographical routing and it should be secured. An attacker can easily manipulate the non- secured location information.
- Flexibility – the WSN are deployed in real-time applications so the dynamic changes may occur by the user and also by the environment. The sensor nodes may have flexibility to adopt these changes.

2. ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS

The routing protocols are classified under two categories Network structure and Protocol operation [1][6]. Flat network routing, Hierarchical network routing, Location based routing are three types of protocols comes under Network structure.

2.1 NETWORK STRUCTURE

2.1.1 Flat Network Routing

All sensor nodes play the same role or functionality. It is a data-centric routing, where the base station sends queries to certain regions and wait for data from the sensors located in the selected region. The SPIN and Directed Diffusion are the protocols follow data-centric routing.

A. SPIN – sensor protocols for information via negotiation. The SPIN assumes nodes in closer have similar data, so the SPIN distributes all the information at each node to all other nodes in the network that do not possess the information. The SPIN performs meta – data negotiations before any data is transmitted so no duplication is sent. SPIN works in time-driven fashion and does not flood the data. Advantage of SPIN is energy savings than flooding and avoids duplication. The Disadvantage of SPIN is it cannot guarantee the delivery of data.

B. Directed Diffusion – The steps in directed diffusion are

- A node broadcasts the interest to the neighbors or base station.
- The gradients are setup to draw data satisfying the query towards the requesting node.
- This process continues until gradients are setup from the source back to the base station
- The best paths are chosen to prevent further flooding.

One drawback of Directed diffusion is that it consumes more network resources for the selection of best route.

C. Rumor Routing – Instead of flooding the entire network route the queries to the nodes that have observed a particular event. When nodes detect an event it adds it in event table and generates an agents. Agents send the information to the requested node. Only one path is maintained between source and destination so it saves considerable energy.

MCFA, Gradient based Routing, IDSQ, CADR, COUGAR, ACQUIRE, Energy aware routing, Routing protocols with random walks are other protocols comes under Flat Network routing.

2.1.2 Hierarchical Network routing

All nodes transmit a message to a node that is in the higher hierarchy level than a sender. Each node aggregates the information so it reduces the communication overhead and conserves more energy. Inturn increases the network lifetime. The hierarchical routing is a two layer routing where one layer selects the cluster heads and the other layer is used for routing.

A. LEACH – Low Energy Adaptive Clustering Hierarchy. In LEACH, the network is randomly divided into clusters and cluster heads are chosen among the cluster nodes in a round robin fashion. The sensor nodes transmit data to cluster heads which transmits the aggregated data to the Base station. The simulation results shows that HCR –Hierarchical cluster based routing is more energy efficient than other routing techniques. LEACH uses a TDMA/CDMA MAC to reduce inter – cluster and intra-cluster collisions.

PEGASIS, TEEN and APTEEN, MECN, SOP, Sensor aggregates routing, VGA, HPAR are several other protocols comes under Hierarchical Network routing.

2.1.3 Location Based Routing Protocol

The protocol uses location information of the neighbors to route the packet to the destination. The control overhead of the algorithm is reduced and routing is optimized. The location of a node is found with GPS (Global Positioning System) and some nodes go to sleep if there is no activity.

A. Geographic Adaptive Fidelity (GAF*)*

GAF is a location-based routing protocol and usually the network area is divided into fixed zones. Inside each zone one sensor is elected to stay awake for a certain period of time and it is responsible for monitoring and reporting data to the base station and then they go to sleep.GAF conserves more energy by turning off the unnecessary nodes.

B. Geographic and Energy Aware Routing (GEAR)

Sensor nodes send the request to only one neighbor towards the destination rather than flooding the entire network. The responses are directed in the same way. GEAR conserves more energy than Directed Diffusion.

MFR, DIR, GEDIR, GOAFR, SPAN are other protocols belong to a location based routing.

2.2 PROTOCOL OPERATION

Negotiation Based Routing, Multipath-based routing, Query based Routing, QOS based routing, coherent based routing are the classification of protocols under protocol operation.

2.2.1 Multipath based routing protocol

The routing protocol uses multiple node-disjoint paths between the sink and source node. When the primary path fails it automatically chooses the alternate path between the source and sink. The path will be changed whenever a better path is identified. The multipath increases the reliability of the network. Directed diffusion uses the multipath routing.

2.2.2 Query based routing

The node sends a query to all other nodes in the network, and the node having the data for requested query will send a response. Directed diffusion and rumor routing is an example of query based routing (probabilistic routing)

2.2.3 Negotiation based routing protocols

SPIN is an appropriate example of negotiation based protocol. The communication decisions are taken between the nodes. The sensor node sends the data to the other nodes which do not posses those data. So duplication of data is avoided in the network.

2.2.4 QoS-based routing

The network has to satisfy three QoS metrics – delay, energy, bandwidth etc. SAR is an example of QoS-based routing. SAR is a table driven multipath protocol. When a node fails a path recomputation is needed. SAR maintains a multiple paths from nodes to base station so when the node fails alternate paths can be used.

2.2.5 Coherent and Non-coherent processing

In a Non coherent data processing node locally processes the raw data before sent to other nodes in the network. The aggregators perform remaining processing.

In the coherent routing minimum processing like time stamping, duplicate suppression is made then forwarded to aggregators.

3. ATTACKS IN WIRELESS SENSOR NETWORK

Attacks are purely classified in to two types, they are active and passive attacks [3].

3.1 ACTIVE ATTACKS

Active attacks gains the physical control of the node and disturb the normal functionality of the network, these can be easily detected. Routing attacks, node replication attacks, denial of service attacks, physical attacks comes under active attacks [4] [5].

3.2 PASSIVE ATTACKS

The passive attacks observe the conversation between the nodes and make an alternation of information without interrupting the communication. Passive attacks cannot be easily detected and it is very dangerous when compare with active attacks, since it is unable to recognize the attacker. Attack against the privacy like monitor and eaves dropping, traffic analysis, camouflage adversaries comes under passive attacks.

3.3 ROUTING ATTACKS

A Variety of network layer attacks have been identified. The attackers observe the communication between the nodes and inject themselves into the path between the source and destination, alter the messages, create routing loops, data loss can occur, packets may be forwarded to a non existent path.

The following are the specific attacks identified in the network layer [5]

1. Spoofed, altered or replayed routing information
2. Selective forwarding
3. Sinkhole attack
4. Sybil attack
5. Wormhole attack
6. Hello flood attack
7. Acknowledgement spoofing

Table 1 summarizes the attacks in routing protocols:

Routing Protocols	Attacks
Flat network routing (Directed diffusion, Rumor Routing)	Selective forwarding, false routing information, tampering, sink holes, sybil attack, hello flood attack , wormhole attack
Hierarchical Routing (LEACH, TEEN, PEGASIS)	Selective forwarding, hello flood attack.
Location Based routing protocol (GAF, SPAN, CEC, AFECA)	False routing information, sybil attack, hello flood attack.

3.3.1 Spoofed altered or replayed routing information.

The false routing information occurs in the location based routing protocol. The attackers can observe the traffic inside the network and alter the complete message or part of it before sending it to the base station. This attack can be done directly or indirectly by the attacker. If the attack is indirect one then it is very difficult to detect such attackers. Some times routing loop can occur (replayed routing information) i.e. the attacker can circulate the information in the particular region of the network and prevent data to reach the destination node.

3.3.2 Selective forwarding

Directed diffusion, rumor routing, LEACH, GPSR all these protocols are vulnerable to selective forwarding attacks. The compromised node just forwards a subset of packet it receives and drops the others. So the neighboring node assumes that path is failed and decides to take another route. This is one kind of black hole attack. This attack is very hard to detect because the adversary will not drop every packet. There may be single malicious node, two consecutive malicious nodes or more than two malicious nodes. Network with single malicious node, selectively forwards the packet. Network with two malicious nodes are difficult to detect packet dropping. Network with one or more malicious node prevents the packet forwarding to the base station.

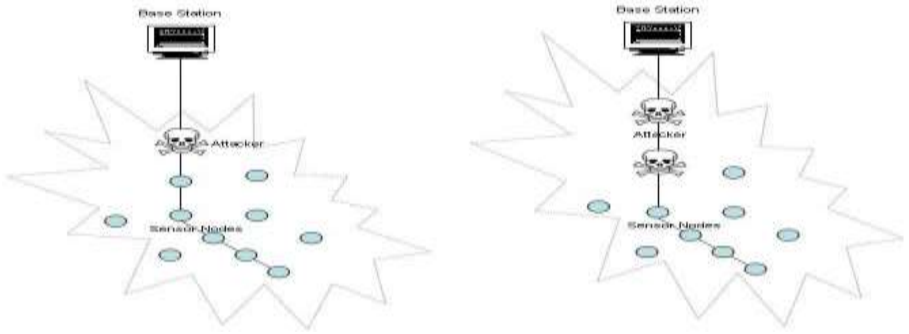
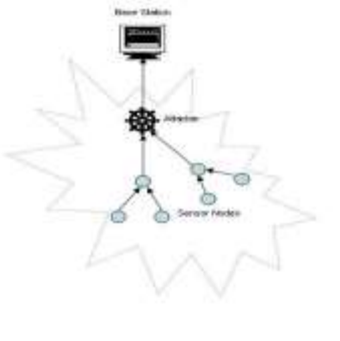


FIG.1 SELECTIVE FORWARDING WITH SINGLE AND MULTIPLE MALICIOUS NODES

3.3.3 Sink hole attack

Directed diffusion, rumor routing are vulnerable to sink hole attack[10]. In the wireless sensor network all the sensor nodes continuously monitor the changes in surroundings and forward to the sink node. The WSN is many to one communication between the sink node and the sensors. So it is greatly vulnerable to the sink hole attack. The compromised node involves itself in the network and tells a sensor that is close to the sink. So all the sensors route the sensitive information to the compromised node. The compromised node can alter the information or replay an advertisement before sending to the base station[11]. The sink hole attack combines with the other attacks like selective forwarding and thus prevents the base station to obtain a complete information and creates a serious threat to higher-level layers of application.



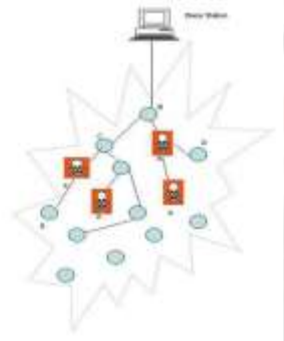


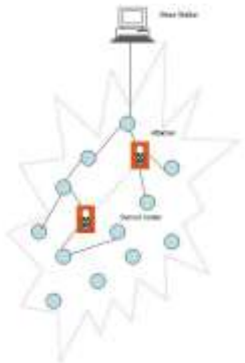
FIG.2 SINKHOLE ATTACK FIG.3 SYBIL ATTACK

3.3.4 Sybil attack

The routing protocols like directed diffusion, rumor routing, location based routing protocols are vulnerable to sybil attack[13]. The single id is shared by multiple sensor nodes at the same time. This attacks many important functions of the network like resource allocation, routing, decrease data integrity etc. Sybil attack is very hard to detect, only when centralized base station is present it prevents the sybil attack on the sensor network.

3.3.5 Worm holes attack

Rumor routing protocols are susceptible to worm hole attack. The worm hole attack places two or more malicious nodes at different locations and tell the network that is the shorter route and data can travel faster than it could on the original network. So all nodes transmit data to the malicious nodes and these nodes retransmit them in the network again and again creating a routing loop. Worm hole can combine with other types of attacks like selective forwarding, sink hole, Eaves dropping. Detection is difficult when combined with sybil attack[14]. The worm hole attack after attracting the traffic it can disturb the routing, data flow, altering data packets etc.



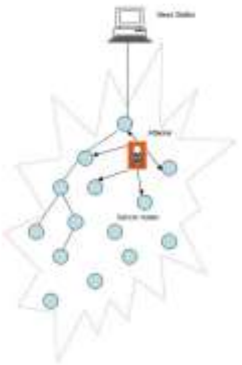


FIG.4 WORM HOLE ATTACK FIG.5 HELLO FLOOD ATTACK

3.3.6 Hello flood attack
Directed diffusion, hierarchical routing, location based routing are susceptible to hello flood attack[16]. In WSN the hello packet is broadcasted to announce itself as a node neighbor. An adversary takes the advantage of this technique and these nodes broadcasts hello packets with enough transmission power and convince every node in the network that the adversary is its neighbor. So all the sensor nodes and base station could use it to transfer data, the adversary node rebroadcast the data it receives, leads to a worm hole attack.

3.3.7 Acknowledgement Spoofing
The malicious node convinces other nodes in the network by telling weak link is strong or some dead node is alive. The source nodes believes the false acknowledgment information and sends data on those weak links results in pack loss or alteration of data.

4. DETECTION, PREVENTION AND AVOIDANCE OF ATTACKS IN WIRELESS SENSOR NETWORKS

4.1 SECURITY MECHANISMS FOR SPOOFED, ALTERED OR REPLAYED ROUTING INFORMATION

Regular monitoring of sensor nodes and dynamic routing will automatically detect and prevents the spoofing attacks. The end – to – end latency increases by the replayed routing information. This can be prevented by implementing time driven protocol. Encryption and authentication by centrally controlled base station could avoid the false message from adversary.

4.2 SECURITY MECHANISM FOR SELECTIVE FORWARDING

Bo Yu , Bin Xiao [8] proposed the detection scheme for selective forwarding attack, each intermediate node sends an alarm packet to the base station, when it detect the misbehavior at downstream (upstream) through multiple hops. To avoid the selective forwarding attack it is necessary to avoid the compromised node by encryption and authentication.

To prevent the selective forwarding attack, the alternate best route has to be calculated on each and every node or at the base station so that alternate route can be accessed from base station.

4.3 SECURITY MECHANISM FOR SINK HOLE ATTACK

Encryption and authentication using a globally shared keys avoids sink hole attack.

EdithC.H.Ngai, Jiangchuan Liu, and Michael R.Lyu [9] proposed a novel algorithm for detecting the intruder in a sink hole attack. The algorithm finds a list of suspected nodes and identifies the intruder through a network flow graph.

4.4 SECURITY MECHANISM FOR SYBIL ATTACK

To defend against sybil attack there are two methods, direct and indirect validation. In direct validation, the node directly tests whether another node identity is valid. In Indirect validation, the verified node is allowed to test node identity.

J. R. Douceur [18], proposed resource testing as a method of direct validation. James Newsome, Elaine Shi, Dawn Song, Adrian Perrig [12], proposed several techniques like random key pre distribution scheme, registration and position verification.

Chris Karlof, David Wagner [5], proposed identities must be verified using public key cryptography but verifying the digital signature is beyond the capabilities of sensor nodes. Another solution to avoid sybil attack is the base station can limit the number of neighbor nodes and can send an error message when a count exceeds it.

4.5 SECURITY MECHANISM FOR WORM HOLE ATTACK

Jackson kwok [19], proposed localization schemes and packet leashes to prevent worm hole attack. The localization system verifies the location of nodes, to conclude that packets are sent by either a node or worm hole. The packet leashes, places a limit on a maximum allowed transmission distance in a network.

L. Hu and D. Evans [20] proposed a technique called directional antennas. In this each couple of nodes has to examine the direction of received signal from its neighbor. The packet has to send only if the directions of both pairs match.

W. Wang, B. Bhargava [21], proposed the network visualization to identify a worm hole attack. All the sensor nodes have to determine the distance of its neighbor by the received signal strength. All sensor nodes sent the distance information to the base station, which calculates a physical topology. The physical topology will be flat if there is no worm hole attack other wise there would be a ‘string’ pulling the different ends of network together.

L. Lazos, R. Poovendran [22], proposed a ‘graph-theoretical’ approach to prevent worm hole attack by a ‘local broadcast keys’ - a message encrypted with a local key cannot be decrypted at another end.

T. Park and K. Shin [24], proposed a protocol to detect a worm hole attack in a static network. It determines whether data packets are forwarded by the neighbor or not.

N. Song, L. Qian, X. Li [23], proposed, the message forwarded by a worm hole are at a higher frequency allows to detect the attack easily.

4.6 SECURITY MECHANISM FOR HELLO FLOOD ATTACK

Md. Abdul Hamid, Md. Mamun-Or-Rashid and Choong Seon Hong [16], proposed a bi-directional verification and multi-path routing to multiple base stations to defend against hello flood attack. In bi-directional verification any two sensor nodes share some common secret keys, so when adversary nodes generate a request keys it is decrypted and verified since the attacker does not know the secret key, it will be prevented from launching the attack.

In multi-path multi-base station data forwarding, there may be no of base stations in the network, each base station has the secret key shared by all the sensor nodes according to the key assignment protocol.

Virendra Pal Singh1, Sweta Jain2 and Jyoti Singhai [15], proposed a technique to detect and prevent the hello flood attack by checking the signal strength. The signal strength of all sensor nodes is assumed to be same in a radio range. If the signal strength varies then it is identified as an attacker.

Chris Karlof, David Wagner [5] proposed a cryptographic technique to prevent a hello flood attack. Other solutions are to check the number of hello messages received by a counter if the no of hello messages are less it is solved first otherwise the request will be solved later. Another method for preventing hello flood attack is to keep time threshold value if the reply is not received under pre defined threshold value then it is treated as an attacker.

4.7 SECURITY MECHANISM FOR ACKNOWLEDGEMENT SPOOFING

The encryption and authentication using a globally shared key avoids the acknowledgement spoofing. Sending the dummy packets periodically can check the nodes are alive or not. So if the attacker sends the dead node is alive it can be easily detected by a base station.

5. CONCLUSION

In this work, a survey was made on the security requirement for WSN and in section 2 several routing techniques has been discussed. Since the knowledge on routing techniques is necessary only when, the attackers can easily be identified and routing techniques can easily be modified according to the attackers. Nowadays all types of wireless networks are easily attacked by the active attackers. So in section 3 analyses was made on the routing attacks specifically. In section 4 security mechanisms proposed by different researches are discussed. Future work is on finding the better security mechanisms for routing attacks without reducing network performance and also modifying the routing techniques to avoid compromised node without increasing in hop count.

REFERENCES

[1] Jamal N.Al-karaki, Ahmed E.Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey".

[2] Muazzam A.Khan,Ghalib A.Shsh,Muhammad Sher "Challenges for Security in Wireless Sensor Networks" in World Academy of Science, Engineering and Technology 80 2011.

[3] Teodor-Grigore Lupu "Main types of Attacks in Wireless Sensor Networks".

[4] Dr.G.Padmavathi, Mrs.D.Shanmugapriya,"A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" in IJCSIS, Vol 4, No.1 &2, 2009.

[5] Chris Karlof, David Wagner," Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures".

[6] Gergely Acs, Levente Buttyan,"A Taxonomy of Routing Protocols for Wireless Sensor Networks" Budapest University of Technology and Economics, Hungary, January 12, 2007.

[7] Ace Dimitrievski , Vera Pejovska , Danco Davcev , "Security Issues and Approaches in WSN".

[8] Bo Yu Bin Xiao," Detecting Selective Forwarding Attacks in Wireless Sensor Networks".

[9] Edith C. H. Ngai, Jiangchuan Liu, and Michael R. Lyu1,"On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks" publication in the IEEE ICC 2006 proceedings.

[10] Ioannis Krontiris, Thanassis Giannetsos, Tassos Dimitriou,"Launching a Sinkhole Attack in Wireless Sensor Networks; the Intruder Side".

[11] Anthonis Papadimitriou,Fabrice Le Fessant,Aline Carneiro Viana,Cigdem Sengul",Cryptographic Protocols to Fight Sinkhole Attacks on Tree-based Routing in Wireless Sensor Networks".

[12] James Newsome, Elaine Shi, Dawn Song, Adrian Perrig,"The Sybil Attack in Sensor Networks: Analysis & Defenses".

[13] Brian Neil Levine, Clay Shields. Boris Margolin,"A Survey of Solutions to the Sybil Attack".

[14] Shalini Jain, Dr.Satbir Jain "Detection and prevention of wormhole attack in mobile adhoc networks ", International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010.

[15] Virendra Pal Singh, Sweta Jain and Jyoti Singhai3 "Hello Flood Attack and its Countermeasures in Wireless SensorNetworks" IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010.

[16] Md. Abdul Hamid, Md. Mamun-Or-Rashid and Choong Seon Hong "Routing Security in Sensor Network: HELLO Flood Attack and Defense", Next-Generation Wireless Systems ICNEWS 2006.

[17] Siddhartha Choubey, Abha Choubey, M.Abhilash3, Kamal K Mehta4,"Defense Mechanisms against Hello Flood Attack in Wireless Sensor Network".

[18] J. R. Douceur. The Sybil attack. In First International Workshop on Peer-to-Peer Systems (IPTPS '02), Mar. 2002.

[19] Jackson Kwok "A Wireless Protocol to Prevent Wormhole Attacks" A Thesis in TCC 402 Presented to The Faculty of the School of Engineering and Applied Science University of Virginia, March 23, 2004.

[20] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in Proceedings of the Network and Distributed System Security Symposium.

[21] W. Wang, B. Bhargava., Visualization of wormholes in sensor networks, Proceedings of the 2004 ACM workshop on Wireless Security, pp. 51-60, 2004.

[22] L. Lazos, R. Poovendran, Serloc: Secure Range-Independent Localization for 21- 30, Wireless Sensor Networks, Proceedings of the ACM Workshop on Wireless Security, October 2004.

[23] N. Song, L. Qian, X. Li, Wormhole Attack Detection in Wireless Ad Hoc Networks: a Statistical Analysis Approach, Parallel and Distributed Processing Symposium, 2005, Proceedings of, 19th IEEE International IPDPS'05, 04-08 April 2005, pp.

[24] T. Park and K. Shin, "LISP: A Lightweight Security Protocol for Wireless Sensor Networks", in proceedings of ACM transaction on Embedded Computing systems, August 2004.