International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 4, April - 2013

Analysis And Overview Of Routing Protocols And Security Attacks In Wireless Sensor Networks

Hemangpriya Shrivastava*1 Sandeep Sahu*2

Shriram Institute of Engineering and Technology,Jabalpur(M.P.),482001,India.

Abstract

The collections of large number of sensor nodes are called wireless sensor networks. It is one of the domineering technologies in near future and also poses the unique challenges for the researchers to related field. Sensor networks are tiny nodes with sensing, computation capability. The fault tolerance, high sensing fidelity, flexibility and rapid deployment are some of the characteristic of sensor network which make it exiting in the field of remote sensing. Though there is another side too. In a very large scale sensor network individual sensors are subject to security compromise. Attacker can overhear the messages sent by another sensor node due to broadcast nature of communication. With increasing requirement of WSN in the areas of military and other areas, the security threats also increases. However the open nature of the wireless communication channels, the lack of infrastructure, the fast deployment practices, and the hostile environments where they may be deployed, make them vulnerable to a wide range of security attacks. The key issues in WSN are security, energy consumption and proper communication .In this paper we surveyed all the possible security attacks and all the geographical routing protocols in WSN .Some possible security attacks in wireless sensor network are Sink hole attack, Sybil attack, selective forwarding attack, wormhole attack and hello flood attack. This paper presents a thorough review of all the routing protocols as well as all these attacks which are given above in WSN.

Keyword-WSN,QOS,C4ISRT,S-GPSR,GPSR,Sybilattck, Sinkhole attack, Black hole attack, Wormhole attack, Hello flood.

1.Introduction

Wireless sensor network is recently emerged as the premier research topic. They have ability to pose many new systems building challenges, Great long-term economic potential and ability to perform our lives. The fundamental issues related to wireless sensor network are quality of service, fault tolerance, energy harvesting etc. The utilization of adaptive power control in IP networks that utilize reactive routing protocols and sleep mode operations more powerful mobile agents QOS to guarantee delivery security mechanism, robustness and fault tolerance.

Now a day WSN has become a good tool for military applications .It involves intrusion detection smart logistic support in an unknown deployed area perimeter monitoring and information gathering .C4ISRT[1] system in military that is command control ,communication ,computing intelligence, surveillance, reconnaissance and targeting systems . For these systems wireless sensor become integral part .Some of the other military application of Sensor networks are – Monitoring friendly ,forces equipment and ammunition, battle field surveillance, reconnaissance of opposing forces terrain ,targeting battle damage assessment and nuclear biological and chemical(NBC)attack detection and reconnaissance. Apart from that the sensor networks are also used for continuous sensing, event ID, location sensing, and local control of actuators. The application areas of WSN are environment, health, home and other commercial applications.

All above applications needed secure and accurate routing of packet in geographical area. We surveyed basically three types of routing protocols in WSN

2. Types of routing protocols

2.1. Data centric protocols

In data centric routing [2] queers are posed for specific data rather than the data from particular node. This type of routing is performed for mete data. The common data centric protocols are given below.

2.1.1. SPIN. The sensor protocol for information via negotiation protocol[3] is a negotiation protocol in

which only the interested neighbor who wants the meta data of sender node, reply with REQ message for the advertisement of senders data.

2.1.2. Shah et al. They propose to use a set of suboptimal paths to increase network lifetime[4] .They said that by using minimum energy path all the time will continuously depletes the energy of nodes on that path. They use the concept of energy metric.

2.1.3. Yao et al. They propose the protocol that observe the network as a huge distributed database system .The key idea behind the protocol is COUGER [5] approach which exploits in networks data aggregation to conserve more energy. The abstraction is supported through an additional query layer that lies between the network and application layer. The data aggregation is performed by a pilot node which is selected by a query plan specified by the same.

2.1.4. Directed diffusion. It is also a query driven protocol .The main aim of directed diffusion[6] at naming all data generated by sensor node by attribute value pair. Other variants of directed diffusion are rumor routing [7] and Gradient-Based Routing (GBR) [8]

2.2. Hierarchical routing protocol

The main aim behind hierarchical routing protocol [7] is to minimize energy consumption. It is achieved by diving nodes into clusters .In which the node which is selected as cluster head will have maximum processing power .The major drawback of this class of protocols is the only that it has increased local communication cost between sensors .And the increased processing cost of information gathered and processed as a cluster head.

2.2.1. LEACH. Low energy adaptive clustering hierarchy [9] is an adaptive clustering base protocol that uses randomized rotation of cluster head to evenly distribute energy load among the sensor node in the network.

2.2.2. PEGASIS. Power efficient gathering in sensor information system [10] is considered as an optimization of leach algorithm. It forms \a chain of sensor nodes rather than make clusters. By third technique each node transmits and receives from only closest node of its neighbors.

2.2.3. TEEN. Threshold sensitive energy efficient sensor network [11] and its adaptive version, ADAPTIVE threshold sensitive energy efficient network APTEEN [12] are like LEACH and by threshold mechanism both designate transmission node.

2.3. Geographic routing or location based routing

The main concept of location based routing is that it takes advantage of local information to make routing techniques more efficient. In this type of protocol the direct neighbors exchange information about their location derived from global positioning system (GPS) devices. Or in infrastructure utilization system by using only local topology information GRP can find new route towards final destination and fast response too for the dynamic topology changes. The energy and bandwidth are preserved as nodes are not required to keep state information beyond a single hop.

2.3.1. GEAR. It uses energy aware and geographically informed neighbor selection heuristic [13] to route a packet towards the destination region.

2.3.2. GAF. It utilizes a virtual grid for gathering and routing messages .It saves energy by turning off unused nodes without compromising any routing fidelity and communications in a multi hop manner [14].

We have given the brief introduction of all the protocols according to their classification, data aggregation, scalability, power usage, QOS, Overhead, Query based and data delivery model in the table given below.

Table 1 Comparison of routing protocols in WSN

Routing protocols	Classification	Data aggregation	Scalability	Power usage	QOS	Overhead	Query based	Data delivery model
SPIN[3]	Flat/Data Centric	yes	limited	limited	no	low	yes	Event Driven
COUGAR[5]	Flat	yes	limited	limited	no	high	yes	Query driven
DD[6]	Flat/Data centric/dest.iniciated	yes	limited	limited	no	low	yes	Demand driven
LEACH[7]	Hierarchical / Dest-initiated /Node-centric	YES	Good	High	No	High	No	Cluster Based
PEGASIS[8]	Hierarchical	No	Good	Maximum	No	Low	No	Chains Based
TEEN[9]	Hierarchical	Yes	Good	High	No	High	No	Active threshold
GEAR[10]	Location	No	Limited	Limited	No	Moderate	No	Demand Driven
GAF[11]	Location	No	Good	Limited	No	Moderate	No	Virtual Grid

2.3.3. GPSR. GPSR [15] is the combination of greedy forwarding and perimeter forwarding for routing the data to the destination. It is a Greedy forwarding routing algorithm in which local minimum problem is introduced and which contains location information of base station and 1-hop neighbor nodes. The rule of GPRS said that it will select the next node which will be progressively closer to the destination node. This method is known as greedy forwarding method. After meeting local minimum problem some authors' adopt graph theories to solve the local minimum problem. Sometimes there is a situation when all the nodes in neighbors are away from the destination node than the base station through which packet is to be routed. Then there will empty region created .That region is called voids. On that situation right hand rule will be applicable which is sometimes called perimeter forwarding, because after that the packet should be forwarded into the given perimeter over void. The two combined method of GPSR is given below-

2.3.3.1. Greedy forwarding. By the GPS server ,source node obtain the information about the geographical position of all the neighbor nodes and the destination nodes' packet can then be routed towards the destination in the greedy mode. In a greedy mode a node selects the neighbor node which is geographically closest to the destination. After that it progressively selects a locally optimal node as the next hope till it can find such neighbor or until the destination is reached. Consider an example shown in fig 4.1. In the given figure, A receives a packet which is to be sending for D. The radio range of A is represented by a white lined circle which is centered at A, and the radius of the arc is equal to the distance between B and D is shown as the thin lined arc about D. Among all it neighbours A forwards packets to B, because the distance between B and D is actually less than that of between D and any node of the A's neighbor. The major advantage of greedy perimeter is it relies only on the knowledge of the forwarding node's immediate neighbors. Thus the amount of memory and the processing in the sensor network is considerably saved and the state requirement is

negligible. Thus GPRS can scale to large number of Wireless Sensor Network and save much amount of energy also.

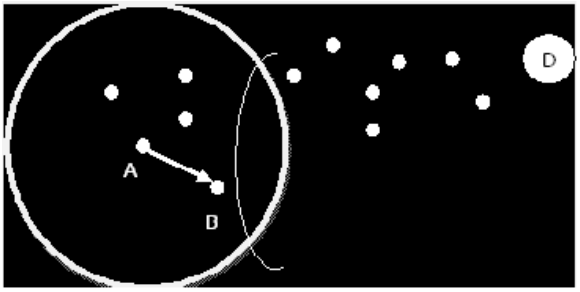

Figure 1. Greedy Forwarding in GPSR

2.3.3.2. Failure of greedy forwarding and Perimeter Forwarding. The failure of greedy forwarding will occur only when due to change of topology move data packet temporarily away from the destination we can understand this by simple example of such topology is shown in fig 4.1.2. In this case, E is closer to D as compared to its neighbors F and C. The thin lined arc about D has a radius equal as compared to the distance between E and D. This is represented by a void as shown in fig 4.1.2. Now there exist two paths via F and via C through which E can route packets towards D. Hence, E has to shift the packet temporarily away from the destination. E then selects the next node according to the right hand rule and the packet follows the path along the perimeter of the void towards the destination and the packet is said to enter into the perimeter mode.

2.3.4. Secured GPSR. As mentioned above GPSR forwards node greedily to the neighbor node which is nearest to destination. We saw that in such type of protocols there is no security mechanism. Thus Samundiswari et al. [16] will give the concept of Secured GPSR for sensor networks. They use the concept of trust levels .In conjunction with the geographical distances are incorporated in the neighborhood table to create the most trusted distance route rather than the default minimal distance.

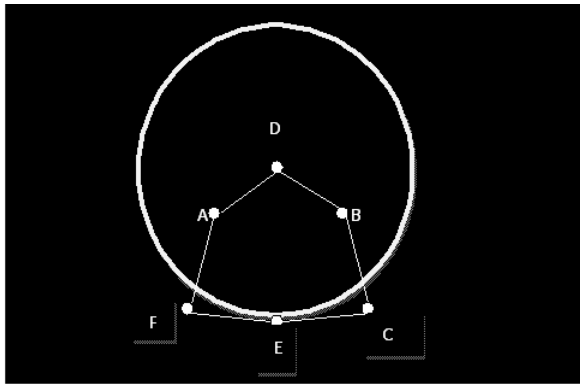

Figure 2.Failure of Greedy forwarding ,' E' is a local minimum in its geographical proximity to 'D'.F and C are farthest from D.

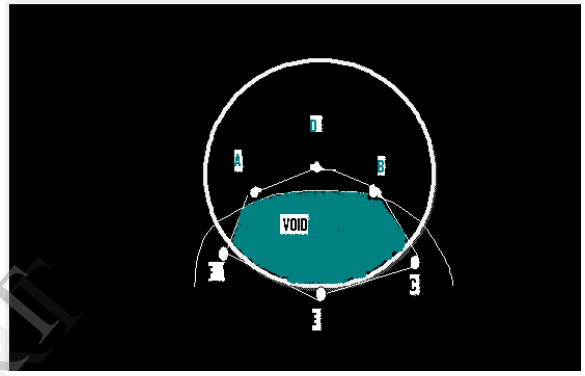

Figure 3. Node E's void with respect to D

An effort-return based trust model issued for computing direct trust in node. The accuracy and sincerity of immediate neighboring nodes is ensured by observing their contribution to packet forwarding mechanism. They implement the trust derivation mechanism; Trust Update Interval (TUI) of each forwarded packet is buffered in the node as (GPSR Agent::buffer packet). The TLC, TUI and DTC initialize to zero. The TUI is a very demanding component of such a trust model. It determines the time a node should wait before assigning a trust level or distrust level to a neighbor based upon the results of an accurate event. After transmitting a packet each node licentiously listens for the neighbor node to forward the packet. If neighbor forwards the packet in proper manner within the Trust update interval, its corresponding trust level is Incremented. However, if the neighboring node modifies the packet in an abrupt manner or does not forward the packet at all, its trust level is decremented. Every time a node transmits a data packet, it immediately brings its receiver into licentious mode (GPSR Agent::tap), so as to eavesdrop its immediate neighbor forwarding the packet. The sending node checks the different fields in the forwarded IP packet for compulsory modifications through a sequence of integrity checks

(GPSR Agent::verify packet integrity). If the integrity checks are successful, it approves that the node has acted in an unselfish manner and so its direct trust count (DTM) is incremented. On the other hand, if the integrity check will be unsuccessful or the forwarding node does not transmit the packet at all, then its related direct trust measure is decremented and the node is treated as malevolent node. The T-GPSR is explained by using flow chart which is illustrated through Figure

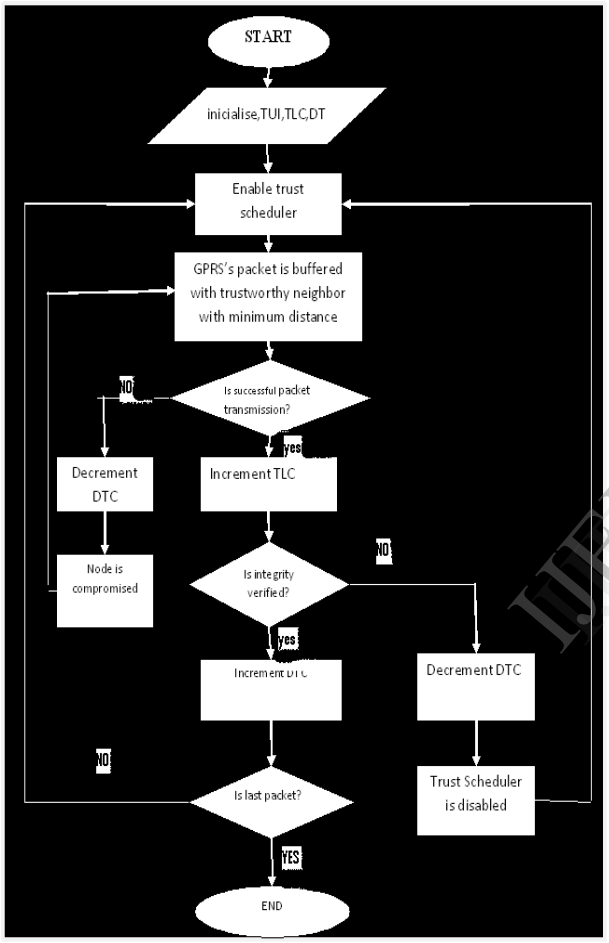

Figure 4. Flowchart of S-GPSR

3. Types of security attacks in geographic routing protocol

3.1. Wormhole attacks

In the wormhole attack a malevolent node tunnels messages received in one part of the network over a low abeyance link and epitomize them in a different part. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to itself, after all it can eavesdrop them in wireless transmission and tunnel them to the cogitate attacker at the opposite end of the wormhole. The tunnel creates the deception that the two end points are very close to each other, by making tunneled packets arrive either sooner or with lesser number of hops compared to the packets sent over normal routes. This allows an attacker to confound the correct operation of the routing protocol, by controlling numerous routes in the network. After that he can use this to perform traffic analysis or selectively drop data traffic. The wormhole attack mainly consists in network layer attacks when the attack is classified according to network protocol stacks. A.A. Pirzada et al. [17] analyzed the creation of the wormhole and pose three ways:

A) Tunneling the packets above the network layer
B) Long Range tunnel using high power transmitters
C) Tunnel creation via wired infrastructure

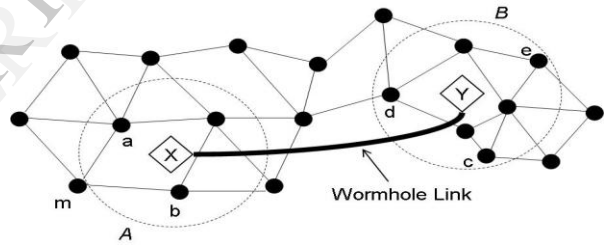

Figure 5. Wormhole in WSN

3.2. Hello flood attack

In many protocol the nodes normally use HELLO packet to check that neighbor node is alive or not or to announce themselves to their neighbors. After receiving that HELLO packet the receiver node assume that it is within the normal range of sender's node. This assumption may be deceitful. When the node with enough transmission power will send the hello packet, then he could convince every node in the network that the rival is its neighbor. Thus, authorized nodes in the network will try to forward their data to the attacking node, those which are out of the boundary, because those nodes will not receive these messages. This attack also can effect on protocols that based on localized information exchange between adjacent nodes like geographical routing protocol. It is not essential for attackers to build lawful traffic due to utilize the HELLO flood attack [18]. They can easily retransmit powerful

overhead packets that every node in the network can received them.

3.3. Black hole and selective forwarding attack

In many case the node, which is malicious by nature will drop or modifies the entire packet. This type of attack is called black hole attack [19]. These types of attack can easily identify in the absence of link, in which the attacking node tries to direct all packages of the network towards itself. In other words it tries to pull all the traffic towards itself. And in fact it tries to introduce itself as the sink. To do this, the attacking node introduces itself the closest node to the sink or considers itself as a node with extraordinary capabilities. It does this to encourage the neighboring nodes to choose the enemy node for routing their data. To overcome this attack we can use the alternate ink to forward the packet. There is special case of black hole attack which is selective forwarding attack. In this type of attack the malevolent node selectively forwards the packet. It will result in deficits of networks efficiency as well as packet loss. This type of selection by adversary is very difficult to detect and resulting the loss of information. There are two forms of attacks found in selective forwarding. One of which node drops all the nodes, and in second it modifies the data. In other words it tries to pull all the traffic towards itself. And in fact it tries to introduce itself as the sink. To do this, the attacking node introduces itself the closest node to the sink or considers itself as a node with extraordinary capabilities. It does this to encourage the neighboring nodes to choose the enemy node for routing their data.

3.4. Sybil attack

In a Sybil attack [20], a malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system. For better understanding of Sybil nodes we surveyed its several forms. Those are given below.

3.4.1. Direct communication Vs indirect communication. In this type of communication sybil attck is for sybil nodes to communicate directly with legitimate nodes.That means the messages sent from sybil nodes are actually sent from one of the malicious devices.In indirect communication no legal node is able to communicate directly with Sybil nodes. Packets sent to a Sybil node are routed through one of these malicious nodes, which show to pass on the message to a Sybil node.

3.4.2. Fabricated vs. Stolen Identities. There are two ways for sybil node for getting identity.In some case the intruder can normally create inconsistantly new sybil identities.For example if every node is identified by 64-bit integer,the attacker can simply assign each sybil node a random 64-bit.Stolen Identities- In a given mechanism there is a process to dentify ligitimate node identities,an attacker cannot fabricate new identities.

3.4.3. Simultanuity. In this mechanism the attacker may try to have his sybil identities all participate in the network at once.A particular hardware entity can only act as one identity at a time,It can through identities to make it appear that they are all present simultaneously.Non-simultaneous –The large number of identities of attacker might be present over a period of time,while only acting as a smaller number of identities at any given time.A particular identity might leave and join multiple times,or the attacker might only use each identity once.

4. Conclusion and future work

We surveyed almost all the routing protocols and security attacks on those protocols. We found that current security approaches for geographic routing should have improved .Thus we will go forward for the extension for secure GPSR. We are looking forward to implement a cost effective and secured defense against Black hole attack and Sybil attack over geographical routing protocol. We are targeting to give better results over S-GPSR and we will try to make our work that it will use minimum of network resources to minimize overhead. Our future work involves designing an algorithm that helps us to estimate the presence or absence of malicious node in an area of a network by using the current information about the network.

5. References

[1]I.F Akyildiz, W.Su, Y.Sankarassubramaniam, E.Cayirci.Wireless sensor networks: a survey, Elsevier, 2001, pp.3-4

[2]Samina Ehsan and bechir hamdaoui. A Survey on Energy-Efficient Routing Techniques with QoS assurances for Wireless multimedia Sensor Networks,IEEE,pp 268-270

[3] W. Heinzelman, J. Kulik, and H. Balakrishnan, “Adaptive Protocols for Information Dissemination in Wireless Sensor Networks,” in *Proc. ACM/IEEE Mobicom Conference (MobiCom ’99), Seattle, WA*, August 1999.

[4] W. R. Shah and J. Rabaey, “Energy Aware Routing for Low Energy Ad Hoc Sensor Networks,” in *Proc. IEEE*

Wireless Communications and Networking Conference (WCNC), Orlando, FL, March 2002.

[5] Y. Yao and J. Gehrke, "The cougar approach to in-network query processing in sensor networks," *SIGMOD Record*.

[6] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking,"
IEEE/ACM Trans. Netw., vol. 11, no. 1, February 2003.

[7] D. Braginsky and D. Estrin, "Rumor Routing Algorithm for Sensor Networks," in *Proc. ACM Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA*, October 2002.

[8] C. Schurgers and M. B. Srivastava, "Energy Efficient Routing in Wireless Sensor Networks," in *Proc. IEEE MILCOM on*
Communication for Network-Centric Operations: Creating the information Force, McLean, VA, 2001.

[9] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energyefficient communication protocol for wireless sensor networks," in *Proc. Hawaii International Conference System Sciences, Hawaii*, January 2000.

[10] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power Efficient Gathering in Sensor Information Systems," in *Proc. IEEE Aerospace Conference, Big Sky, Montana*, March 2002.

[11] A. Manjeshwar and D. P. Agrawal, "TEEN: A Protocol For Enhanced Efficiency in Wireless Sensor Networks," in *Proc. 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA*, April 2001.

[12], "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks," in *Proc. International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, Ft. Lauderdale, Fl*, April 2002.

[13] Y. Yu, D. Estrin, and R. Govindan, "Geographical and Energy Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks," UCLA Computer Science Department Technical Report UCLA-CSD TR-010023, Tech. Rep., May 2001.

[14] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed Energy Conservation for Ad-hoc Routing," in *Proc. ACM/IEEE MOBICOM 2001*, 2001.

[15] B. Karp and H. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*. ACM Press, 2000,

[16] A. A. Pirzada and C. McDonald. Trusted Greedy Perimeter Stateless Routing, IEEE, pp-206-211, 2007

[17]A. A. Pirzada, and C. McDonald. Circumventing Sinkholes and Wormholes in Wireless Sensor Networks. International Work-shop on
Wireless Ad Hoc networks, 2005(5):pp. 132-150.

[18] C. Karlof and D.Wagner, Secure routing in wireless sensor networks: Attacks and countermeasures, Elsevier AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1(2):293-315, September 2003.

[19] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks," in *Proc. ACM/IEEE Mobicom Conference (MobiCom '99), Seattle, WA*, August 1999.

[20] James newsome, Elaine shi, Dawn song, Adrian perrig,"TheSybilAttackinSensorNetworks:
Analysis&Defenses", in *IPSN*, 2004