Secure and Energy Routing Protocol with situation aware for Wireless Sensor Networks

B Yasasvi, Dr. G.Naga Rama Devi

B yasasvi PG Scholar, Dept of CSE, CREC, Tirupati, AP, India
Dr. G.Naga Rama Devi Professor & HOD, Dept. of CSE, CREC, Tirupati, AP, India

---*****---

Abstract -*Wireless sensor network (WSN) typically has energy consumption restriction. Designing energy-aware routing protocol can significantly reduce energy consumption in WSNs. Energy-aware routing protocols can be classified into two categories, energy savers and energy balancers. Energy saving protocols are used to minimize the overall energy consumed by a WSN, while energy balancing protocols attempt to efficiently distribute the consumption of energy throughout the network. In general terms, energy saving protocols are not necessarily good at balancing energy consumption and energy balancing protocols are not always good at reducing energy consumption. we propose an energy-aware routing protocol for query-based applications in WSNs, which offers a good trade-off between traditional energy balancing and energy saving objectives and supports a soft real time packet delivery. This is achieved by means of fuzzy sets and learning automata techniques along with zonal broadcasting to decrease total energy consumption. We then discover that the energy consumption is severely disproportional to the uniform energy deployment for the given network topology, which greatly reduces the lifetime of the sensor networks to optimize the lifetime and message delivery ratio under the same energy resource and security requirement*

Keywords:*Energy-distance awareness, Link failure detection, Accuracy*

1 . INTRODUCTION

Wireless sensor networks (WSNs) have worldwide interest in these years. Advances in Microelectronic Systems and low power radio technology have created low cost, low power, multi-functional sensors devices, which can sense, measure and the information is collected from the environment and transmits the sensed data to the user by a radio transceiver. A battery can be used by the sensor node as a main power source and harvest power from the environment like solar panels as a secondary power supply An unstructured wireless sensor network is a network that contains a dense collection of sensor nodes that can be accessed by the attackers like laptops or their equivalent. They may have greater battery power, a more effective CPU, a high- power radio transmitter, or a sensitive antenna and can do more than an attacker with automatically organized to form an ad-hoc multi-hop network that can communicate with each other .On the other hand, a structured WSN deploys all or only some the sensor nodes in a pre-planned manner thus, it has a lower network maintenance and management cost .WSNs can be used in many applications like military target tracking ,surveillance, natural disaster relief, biomedical health monitoring, environment exploration and agricultural industry [5]. The architecture is commonly used WSN is as depicted in figure 1. Wireless sensor networks like any wireless technology are adaptable to several security attacks due to the broadcast nature of transmission medium

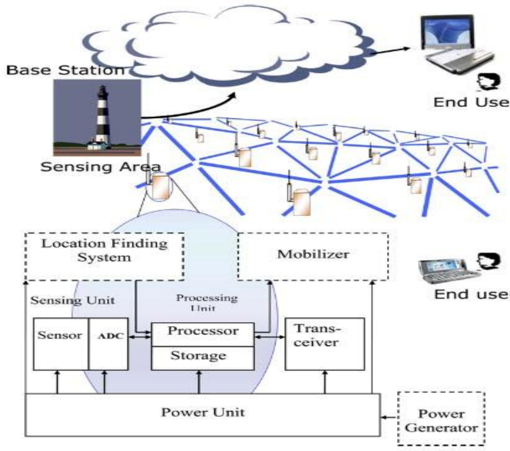

Fig.1 Thearchitectureof commonlyused inWSN

There are constraints in incorporating security intoa wireless sensor networks such as limitations in storage, communication, computation, and processing capabilities. To Design a security protocol these limitations we must understand and achieve acceptable performance with security measures to meet the needs of an application.

2 . WORKING MODEL

Attacks on WSNs can be classified to mote-class attacks and laptop-class attacks. In the mote-class attacks, the intruder has access to a few sensor nodes with similar capabilities. On the other hands, a laptop-class more powerful devices might be

only ordinary sensor nodes [3]. Another classification in attacks on wireless sensor network is based on the outsider or insider attacks Another classification in attacks on WSNs is based on the outsider or insider attacks .In insider attack a compromised node was captured by an opponent and may possess all the secret keys and be capable of participating in the communications and disturbing the network. In contrast, outsider attacks, where the attacker has no special access to the sensor network. Outsider attacks are reached by unauthorized nodes that can easily eavesdrop on the packets exchanged between sensor nodes due to the shared wireless medium [2]. Based on the network layers cites another classification of attacks on WSNs. Attacks at physical layer: In physical layer jamming is one of the most important attack . Aiming at interfering with normal operations, an intruders may transmit continuously radio signals on a wireless channel. An attacker can send high-energy signals in order to effectively block wireless medium and also to prevent sensor nodes from communicating. This can lead to Denial-of-Service(DOS) attacks at the physical layers & also attacks at link layer: The functionality of link layer protocols is to coordinate neighboring nodes to access shared wireless channels and link abstraction is provided to upper layers.Intruders can deliberately violate predefined protocol behaviors at link layer. For example, attackers may induce collisions by disrupting a packet, which leads to exhaustion of nodes' battery by repeated retransmissions, or cause unfairness by misusing a cooperative MAC layer priority scheme. All these can lead to DOS attacks at the link layers. Attacks at network layer: In wireless sensor networks, attacks at routing layer may take many forms. This kind of attacks will be discussed below. Attacks targeting at WSN services and applications: basically, to prevent this kind of attack localization and aggregation are used

3.ATTACKSONROUTINGPROTOCOLSIN WIRELESSSENSORNETWORKS SOME OFNETWORKLAYERATTACKSON WIRELESS SENSOR NETWORKSARELISTEDASFOLLOW:

3.1Eavesdropping- The transport medium in wireless sensor network use broadcasting feature, so any adversary with a strong receiver could eavesdrop and obstruct transmitted data. Information like location of node, Message IDs, Node intrusion detection system, timestamps, application specific information can be retrieve by an intruder. To prevent these problems we should use strong encryption techniques [1].

3.2 Denialofservice- In a Denial-of-Service (DOS) attack, an opponent attempts to disrupt, corrupt or destroy a network. It reduces or a network's capacity is eliminated to perform its expected function [2].

3.3Messagetampering -Malicious nodes are tamper with the received messages thereby altering the information to be forwarded to the destination. The Cyclic Redundancy Code (CRC) would be computed at the destination side. The redundancy check fails and it would result in dropping the packet. If the Cyclic Redundancy code check was successful then the destination node would accept wrong information [2].By altering or replaying routed information, false messages can be generated, routing loops can be created, latency of the network can also be increased, etc. The motivation for mounting a replay attack is to encroach on the authenticity of the communication in WSNs [7].

3.4 Selectiveforwarding -In a selective forwarding attack, malignant nodes may refuse to forward certain messages and simply drop them, ensuring that they are not generated further. A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet . By this, neighboring nodes will conclude that it has failed and decide to seek another route. A more important form of this attack is when an adversary selectively forwards packets. An opponent interested in suppressing packets beginning from a select few nodes can reliably forward the remaining traffic and limit suspicion of its wrong doing. Selective forwarding attacks are typically most effective when the attacker is explicitly included on the path of a data flow. However, it is possible an adversary overhearing a flow passing through neighboring nodes might be able to match selective forwarding by jamming or causing a collision on each forwarded packet of interest [3].

3.5Directeddiffusion -As [7] cites, Directed Diffusion is a data centric A single adversary can use the Sybil attack against her neighbors even in the multipath version. A neighbor will be convinced it is maximizing diversity by reinforcing its next most preferred neighbor but not on the primary flow when in fact this neighbor is an alternate identity of adversary [3].

3.6 Tiny OSbeaconing -This protocol builds a spanning tree that has a base station as the parent for all the nodes in the network. Periodically the base station broadcasts a route that updates to neighbors which in turn they broadcast it to their neighboring nodes. All nodes receiving the update is marked as the base station as its parent and rebroadcast the update. The algorithm continues repeatedly with each node marking its parent as the first node from which it hears a routing update. All packets that are received or generated by a node are forwarded to its parent until they reach the base station [3].As [7] and [3] show, the simplicity of this protocol makes it susceptible to all the attacks discussed in the previous section. Since routing updates are not authenticated, as it is possible for any node to claim to be a base station and can become the parent of all nodes in the network. An authenticated routing updates will prevent an adversary from claiming to be a base station, but a powerful laptop class opponent can still carry out HELLO flood attacks by transmitting a high power message to all the nodes and by making every node to mark the opponent as the parent node. An adversary interested in eaves dropping on, modifying, or suppressing packets in a particular area can be done by mounting a combined wormhole or sinkhole attack. The opponent first creates a wormhole between two colluding laptop-class nodes, one near the base station and one near the targeted area.First node forwards authenticated routing updates to the second through the wormhole and rebroadcasts the routing update in the targeted area. Since the routing update through the wormhole willlikelyreachthetargetedarea considerably faster,thesecondnodewillcreatea largeroutingsub-treeinthetargeted areawithitself astheroot[3]. AsyoucanseeinFigure 6itmight causetoselectiveforwardingattack. Protocolfordrawinginformation outofasensor network. Thebasestationasksfordataby broadcasting interests.Aninterestisataskrequest thatneedstobedonebythenetwork. Among the route,nodeskeep propagatingtheinterestsuntil the nodes that can satisfy theinterests arereached. Each node that receives the interests sets up a gradient toward the origin node. A gradient contains an attribute value & direction. As shown in Figure 5 when node B receives an interest from node A, it includes A(Δ) in its gradient. When the node C receives an interest from node A through node B, it includes B(2Δ) in its gradient. On the other hand, when node C receives an interest from node A, it includes A(Δ) in its gradient. When the data matches the interest (event), path of information, flows to the base station at low data rate. Then the base station recursively reinforces one or more neighbors to reply at a higher data rate. Alternatively, paths may be negatively reinforced aswell. When sources begin to generate data events, an adversary node might attack a data flow and cause to flow suppression. It is an instance of denial-of-service attack. The easiest way to suppress a flow is to spoof negative and positive reinforcements.It can also influence the path taken by a data flow. For instance, after receiving and rebroadcasting an interest, an adversary is interested in directing the resulting flow of events through herself would strongly reinforce the nodes to which interest was sent while spoofing high rate, low latency events to the nodes from which the interest was received. By using the above attack to insert herself onto the path taken by a flow of events, an adversary can gain full control of the flow. That can modify and selectively forward packets of her choosing [3]. On the other hand a laptop-class adversary can exert great influence on the topology by creating a wormhole between one node that located next a base station and other node located close to where events are likely to be generated. Interests advertised by the base station are sent through the wormhole [7]. [3] Shows that the combination of the positive and negative reinforcements pushes the data flows away from the base station and towards the resulting sinkhole..

3.7*Geographicrouting* -Geographic and Energy Aware Routing (GEAR) [9] & Greedy Perimeter Stateless Routing (GPSR) [10] use nodes positions & are informed neighbor selection heuristics and also explicit geographic packet destinations to efficiently disseminate queries and route replies in the sensor network. Greedy Perimeter Stateless Routing uses greedy forwarding at each hop is routing each packet to the neighbor closest to the destination. During the routing, when some holes appear and greedy forwarding becomes impossible, Greedy Perimeter Stateless Routing recovers by routing around the perimeter of the void. One of the GRPS problems is that packets along a single flow will always use the same nodes for the routing of each packet, leading to uneven energy consumption.

4 CONCLUSION

So, security problems at routing layer have to be resolved before their deployment in real world situations. A secure routing protocol must possess preventive measures against the known attacks. Secure Sensor Network Routing protocol provides good security against all known attacks. On detection of any suspicious activity of a malicious node recovery mechanisms should be triggered. Stability of the network should not be drastically disturbed even in the presence of the malicious node. Some secure routing protocols were explained and on implementing these protocols in particular operating system environment, it has been observed that the performance overhead is within acceptable limits compared to the level of security achieved

5 REFERENCES

[1] J. Yick, B. Mukherjee, and D. Ghosal.,*Wireless Sensor* Network Survey, 2008.
[2] R. El-Kaissi, A. Kayssi, A. Chehab, and Z. Dawy., DAWWSEN: A Defence mechanism Against Wormhole attacks in Wireless Sensor Networks.
[3] C. Karlof and D. Wagner, Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, University of California at Berkeley.
[4] J. Paul Walters, Z. Liang, W. Shi, and V. Chaudhary, Wireless Sensor Network Security: A Survey, Department
[5] S. Tripathy and S. Nandi, Defense against outside attacks
in wireless sensor networks, Department of Information Technology, North Eastern Hill University, October 2007.

[6] B. Sun, Y. Xiao, Ch. Chih Li, T. Andrew Yang, Security co-existence of wireless sensor networks and RFID for pervasive computing, Department of Computer Science, Lamar University, USA.
[7] S. Shanmugham, Secure Routing in Wireless Sensor

Networks Scholarly Paper Advisor: Dr. Jens-Peter Kaps.
[8] C. Intanagonwiwat, R. Govindan, and D. Estrin, Directed
diffusion: A scalable and robust communication paradigm
for sensor networks, in Proceedings of the Sixth Annual
International Conference on Mobile Computing and
Networks, August 2000. [9] Y. Yu, R. Govindan, and D. Estrin, Geographical andenergy aware routing: A recursive data dissemination
protocol for wireless sensor networks, University of
California at Los Angeles Computer Science Department,
May 2001.
[10] B. Karp and H. T. Kung, GPSR: greedy perimeter stateless
routing for wireless networks, in Mobile Computing and
Networking, 2000.
[11] D. Braginsky and D. Estrin, *Rumour routing algorithm for*
sensor networks, in First ACM International Workshop on
Wireless Sensor Networks and Applications, 2002.
[12] J. Wang, *ns-2 Tutorial,*Multimedia Networking Group,
The Department of Computer Science