A New Approach For Managing Maximum Energy And Malicious Attack Detection In WSN

Dr. V.Selvi , R.Chinthamani

Abstract: This paper deals about the energy consumption of the entire sensor network by taking into account of various constraints of energy consuming constituents of the network. Then increasing the overall lifetime of various topology of the wireless sensor networks by taking in to account the interconnection between energy consuming constituents and the most important parameters. Determining the effect of energy consuming constituents and their prevalent parameters based on overall energy consumption in WSN.

Index Terms: WSN, malicious attack, energy consumption, Blackhole Attack, Grayhole Attack, Packet Dropping Attacks, Sinkhole Attack

1. INTRODUCTION

THE development of wireless sensor networks (WSNs) has recently opened up a new and interesting area for the creation of new types of applications. WSNs consist of a large number of small sensing nodes that monitor their environment, process data if necessary and send/receive processed data to/from other sensing nodes. These sensing nodes, distributed in the environment, are connected to a sink node – in centralised networks – or to other sensing nodes via a network. In centralised networks, the sink collects sensor data to be used by the end user. In many cases, the sink is also capable of activating sensing nodes via broadcasting, by sending network policy and control information. As with other networks, there are three common design challenges that highly influence the connectivity and productivity of the entire network: (1) using network protocols to minimise control and data packets, (2) selecting the best topology by positioning nodes in the right places, and (3) deploying a routing algorithm that effectively passes data through the network from the origin node to destination node/nodes. Distribution of nodes in the environment can be non-structural or structural. The former is used when there is no control of nodes after distribution, and their only role is to monitor the environment, process the data and build the network by finding and connecting to their neighbours. In the latter, however, the position of each node (both sensing and sink) is clear in advance.

I.A.Wireless Sensor Network (WSN) requirements

It is desirable to prolong the lifetime of the network because sensors are not accessible after deployment. Network size is mostly defined in applications of a larger network is of interest as it covers more area and therefore monitors more events. A faulty network uses resources to generate incomplete data. At the sensor level, it means the monitoring of the environment is broken and many events may be missed. In transmission to the sink, it means packet loss is high; in both cases, the knowledge of the environment is incomplete and therefore the gathered data is not reliable.

These requirements dictate the following criteria in communication protocols:

A.Lower energy consumption: as a direct consequence of the requirement for longer sensor lifetimes, the communication between these sensors (and sink) must slowly consume the available energy, as the majority of a sensors energy is consumed in communication.

B.Compatible with multi-hop communication: typically, sensors avoid direct communication with the sink (as energy usage is proportional to the square of distance); instead, it is preferred that sensors use other sensors as hops to communicate.

C.Scalability: the communication protocol must be reliable in terms of establishing and keeping connectivity among sensors. This protocol must perform as normal when the size of the network becomes larger.

D. Reliability: reliable data transmission in term of packet loss is one of the main concerns to provide a high degree of efficiency in monitoring and control systems.

2. LITERATURE SURVEY

Because of the low cost and light weight of wireless sensors, they are a key device for monitoring systems. However, the short lifetime of these devices, supplying their power via batteries or other limited sources, means that they cannot offer a long-lasting monitoring service. Thus, energy is a critical issue for sensor lifetime. Generally, sensors consume energy when they do individual operations such as data sensing and processing, or group-based operations such as running different communication protocols. There are also several methods for producing energy, but they cannot eliminate the need for energy management. In most situations, these techniques increase the complexity of systems and require new methods for energy management.

II.A. Energy consumption in WSN

WSN sensors, usually deployed in non-accessible environment, are powered using small batteries along with techniques for power harvesting; replacing batteries is not an option. Relying on a battery not only limits the sensor's lifetime but also makes efficient design and management of WSNs a real challenge. The limitation of energy supply, however, has inspired a lot of the research on WSNs at all layers of the protocol stack. Network architectures, such as OSI and Internet, are basically functional models organised as layers where a layer provides services to the layer above (e.g. the application layer provides services to the end users). A network is often evaluated in terms of the quality of its service

- *Dr.(Mrs.)V.Selvi, Assistant Professor in Department of Computer Science Mother Teresa Women's University, Kodaikanal, Tamilnadu, India, PH.9442648983 E-mail: selvigiri.s@gmail.com*
- *Mrs.R.Chinthamani is currently pursuing Ph.d in computer science in*
- *Mother Teresa Women's University, Kodaikanal, Tamilnadu, India,*
- *PH.9751136550 E-mail:sindhuvelmukull@gmail.com*

parameters, such as delay, throughput, jitter, availability, reliability and even security. However, when it comes to energy consumption (EC), one often encounters difficulty, as evaluation and optimization of the network as a comprehensive model that takes the EC into account hardly exists. Generally, researchers focus on the traditional network architecture and try to minimise a specific component of a single layer, with the hope that the overall EC of the network is reduced without regard for other components or layers. This is not an ideal situation, where one does not know how a single component fits within the overall energy picture of an entire wireless sensor network. Most current energy minimisation models focus on sending and receiving data, while other parameters are neglected, the power consumption model focused on the cost of sending and receiving data and deduced the upper limit of the energy efficiency of single hop distance. This approach considers an intermediate node between source and destination so that the retransmission will save the energy. Other approaches evaluate the energy efficiency of wireless sensor networks by using the power consumption. Since wireless networks have different specifications and challenges, the traditional network architecture cannot satisfy them. The cross layer idea was created to provide a flexible network architecture for wireless networks. The key idea in cross-layer design is to allow enhanced information sharing and dependence between the different layers of the protocol stack .

II.B.Physical Layer

Communication between wireless sensor nodes needs a radio connection as a physical layer in which energy is consumed when the radio sends or receives data. The physical layer involves modulating and coding data in the transmitter, and then in the receiver this layer must optimally decode the data. The radio channel has three modes: idle, sleep and active. Thus, the key to effective energy management is to switch the radio off when the radio channel is idle; to consume less energy, it is important to minimise the time and energy to switch between different modes and transmit and receive states. Furthermore, a low-power listening approach may operate at the physical layer, in which the basic idea is to periodically turn on the receiver to sample the incoming data. This duty-cycle approach reduces the idle listening overhead in the network. Moreover, the energy consumption of the radio channel for sending and receiving data is equal; consequently, energy efficient MAC protocols have to maximise the sleep time of sensor. Due to real-time monitoring and interaction with different parts of a sensing node, the operating System (OS) is probably the best place to optimise and manage energy consumption of a WSN at the node level. Perhaps one of the best known techniques at the OS kernel level for minimising energy consumption in the anode is processing unit scheduling by Dynamic Voltage-Frequency Scaling (DVFS). This technique allocates CPU time to tasks and manipulates the CPU power states. In other words, tasks are executed at different frequencies, where lower frequencies mean less power consumption, and the CPU is moved to the lowest power state when there is no task to execute. Parallel thread processing techniques can be useful to reduce the energy usage of a nodes processor; for instance, in a WSN with cluster-based infrastructure, cluster heads become responsible for collecting data and executing the necessity computation operations. Clustering is another technique to minimise energy consumption with a guarantee of deadline constraints. To choose the cluster head candidates; first, for each data collection round, the ratio of initial energy level to the average initial energy of the network is calculated; then, based on these values the cluster head candidates are selected. The node with more resources is picked for data transmission. Clustering, however, has a technical limitation: it can only be used in wireless sensor clusters where all sensors are equipped with DVS processors and have computation ability.

II.C. Link Layer

With regards to energy consumption, the link layer has received a remarkable amount of attention, mainly in energy-aware routing where the aim is to minimise transmission power by multi-hop data transmission instead of direct sensor-link communication. Power consumption in this layer takes into account the consumed energy due to collisions between the radio transmissions of nodes, unnecessary active states due to keeping receivers in the active mode instead of switching to other modes, and the energy required to move from one mode to another mode in the radio circuit. A sensor consumes a large amount of energy during data transmission through three major activities: transmission, reception, and being idle. One study showed that the ratio of power consumption in a processor (including CPU, memory) compared to the radio for the sensor nodes alters from 1:12.5 when both processor and radio are in sleep mode, to 1:4.76 when both are in active mode. As the largest energy consumer in a sensor, radio should play an important role in managing energy consumption and extending sensor lifetime. The problem of energy-efficient reliable wireless communication in the presence of unreliable or lossy wireless link layers in multi-hop wireless networks. Their main focus was on single path routing. The effect of lossy links on energy efficient routing and solved the problem of finding the minimum energy paths in the hop-by-hop retransmission model. However, they all followed a conventional design principle in the network layer of wired networks: after the best path(s) between a source and destination is (are) calculated, all data flows from source and destination follow the selected path(s) until the path is updated after certain topology management update period. ExOR challenged this conventional design principle in the network layer.MAC-independent opportunistic routing protocol. It randomly mixes packets before forwarding them. This randomness ensures that routers that hear the same transmission do not forward the same packets.

II.D. MAC Layer

The problem of how to efficiently employ the residual energy of sensors has been the main concern in designing and developing MAC protocols for WSNs. In this layer, the major energy drift results from collision, control packet overhead, idle listening and overhearing, in which the former plays an undeniable role in designing and choosing energy-efficient MAC protocols in wireless networks. Among popular protocols, two are suitable for this case: time division multiple access (TDMA), and code division multiple access (CDMA). As stated before, one of the approaches to save energy in the link layer is to switch the radio to sleep mode. To take advantage of this opportunity, the link layer requires a time-based medium sharing, e.g., TDMA, with accurate clock synchronisation to properly schedule state transitions; an alternative is to use two

radios to separate channels for data and control messages. TDMA and similar approaches, however, are not suitable for many application in WSNs even though they stop medium contention and reduce energy consumption. Since scheduling time slots is NP hard problem, TDMA and time-based medium sharing approaches do not scale properly. Moreover, these approaches often adapt slowly to changes in the traffic flow and density due to the need for pre-scheduling control messages. CDMA is a promising MAC protocol for most wireless sensor network applications in terms of avoiding collision and supporting bounded delay; however, implementing the original CDMA protocol requires significant changes in the design of sensors. For instance, this protocol needs a large memory to store the codes of all delayed sensors, which is in contrast to the small memory nature of sensors and therefore limits the scalability of CDMA. The transmission time of a message is also lengthened, resulting in an increase in energy consumption, due to the bit encoding part of CDMA. As a result of these limitations, in addition to the circuit complexity and cost of the radio circuit, the designer is required to use only a part of the CDMA protocol to allow a practical implementation of small inexpensive sensor devices, as well as to consume only a small portion of the sensors' energy.

II.E. Network Layer

The network layer consists of a few parts, each one involving different techniques to reduce energy consumption of the network and ultimately improve its lifetime; this section studies these strategies. Briefly, there are a few easy techniques to reduce communication load and therefore consume less energy: among them are decreasing the amount of transmitted data, reducing the number of reporting sensors, and shortening the communication range, to name a few. Since there are different types of nodes in a network and each one has its own energy requirement, assigning energy according to requirement makes it possible to avoid the wastage of residual energy. Non-uniform energy assignment achieves a balance between energy efficiency and energy balance simultaneously. Despite its benefit, monitoring the energy requirement of each node and assigning an appropriate task is very difficult. Generally, sensors have a high degree of cooperation in nature.

II.F. Topology

Determining the best topology among nodes in order to provide a connected network for routing packets to the destination is a significant operation in WSNs. There are several factors that are important in selecting a suitable topology, such as energy efficient deployment and maintenance during the network lifetime, so that the network achieves maximum connectivity with minimum energy consumption. Topology control protocols aim to establish resilient network topology at the same time as minimising the energy consumption in establishing and maintaining the topology. A number of challenges, including duty cycle control of redundant nodes, connectivity maintenance, self-configuration and redundancy identification in localised and distributed fashion.Two significant methods for tackling these challenges are Geographic Fidelity (GAF) and Cluster-based Energy Conservation (CEC) protocols. GAF uses a nodes location information, determined by a GPS, to configure redundant nodes and configures them into small groups using localised and distributed algorithms. CEC has the same fundamental operation but does not depend on location information and radio propagation. These two methods in the same situation. The results show that CEC consumes half of the energy used in GAF protocols. In contrast, when the nodes move frequently, CEC turns off the nodes more often and consequently consumes more energy than GAF. Therefore, GAF is more efficient than CEC in high mobility environments. A new approach was proposed to reduce protocol overheads created by the CEC protocol and the energy consumption of GPS-attached sensors. In this approach, an energy-rich node such as a base station informs the sensors about their cluster ID and cluster area by sending a sweeping beacon. Therefore nodes have information about which cluster they belong to and hence they do not need to carry a GPS. In one of the study the author compared balanced and progressive topologies for sensor networks. Both the balanced and progressive topologies provided energy efficiency, but the best choice depended on the network size. Various kinds of topology, such as tree, mesh, clustered, ad-hoc, and others, provide a virtual backbone for routing in WSNs. The influence of different types of mesh topologies (2D and 3D topologies with different numbers of neighbours) on the power dissipated. According to their results, “increasing the number of neighbours decreases the number of transmission and total power dissipated in the system.” Their main point was that selecting a suitable topology is important as it can support more energy-efficient routing strategies. An online multipath topology management algorithm was presented; for a given topology management request, their technique maximises the lifetime of the network by fair distribution of source to sink traffic along a set of paths. Fuzzy membership functions were applied to the distance between nodes and the nodes residual energy to form an edge weight function in a multipath topology. A better lifetime for the multipath scheme over a single-path fuzzy topology management scheme and online maximum lifetime heuristic using extensive simulation on a variety of network scenarios. Dijkstra to minimise energy consumption in WSN. Under the assumption that energy consumption is proportional to the number of hops, ESRAD formulates energy consumption at both the node and edge and engages Dijkstra to find the shortest paths with the least energy consumption. After categorising the most common WSN multicast procedures based on the geographic position of a target group, the authors presented an algorithm based on Dijkstra for discovering the shortest energy-efficient paths via nodes that provide the maximum geographical advance towards sinks. This algorithm is based on the assumption of availability of the position of the current node, nodes in its neighbourhood (in the radio range of the node) and the location of associated sinks. An algorithm that generates the minimum length multicast tree to send data from one node to multiple sinks in a WSN.The Toward Source Tree (TST) algorithm, it focuses on minimising the number of hops, one of the most important factors in wireless sensor networks, by producing an energy efficient multicast tree with a low complexity. A comparison of energy consumption between chain, grid and random topologies was studied in. The comparison revealed that grid topology had the highest energy consumption followed by random and chain topologies, in that order; chain topology also showed better packet delivery rate than the others. In fact, grid topology had the worst performance in both energy consumption and packet delivery rate.

II.G.Congestion Control

Congestion control algorithms used for wired networks are not appropriate for wireless networks, as packets need to be retransmitted and additional energy has to be consumed. A TCP-like congestion control in a wireless network. As a result, that the throughput drops rapidly when the traffic load increases beyond a certain optimal level due to congestion and packet collision. An alternative method called a hop-by-hop congestion control based on a backpressure mechanism. In this approach, the input flow is maintained below the output flow. This means that if the previous forwarded packet is overheard, the next packet may then be sent. According to the simulations, the approach is successful in increasing the network throughput and decreasing the delay and the retransmission load in different topologies compared to other existing protocols.

II.H. Application Layer

The centrepiece of this layer is an aggregator, which combines data arriving from different nodes, removes redundant data and compresses it before transmission to the intended destination, recalling that reducing the number of transmissions conserves energy. Generally, routing in WSNs considers data aggregation at some nodes. Similarly, for data aggregation, the routing protocol plays an essential role; in cluster-based protocols, cluster head nodes play the role of aggregator to compress data arriving, aggregate data and perform in-network processing. Data aggregation techniques are tied to the method used to generate data in sensors and route packets through the network. Before forwarding to the sink, generated data from different sensors can be processed together. First, data from different nodes are fused together, then processed locally to remove redundant information and finally transmitted. Fusing data from different nodes or in general aggregating data requires the WSNs to be time-synchronised. A protocol at the routing level is required for proper data-gathering; this protocol is formulated to configure the network and collect information from the environment. In each round of data gathering, sensors (nodes) collect data from the environment and send them to the sink. In a more robust way, data fusion is used to combine several unreliable data measurements to produce a more accurate signal (i.e., enhancing the common signal and reducing the uncorrelated noise). The ultimate goal is to consume less energy while transmitting all the data to the sink in order to improve the lifetime of the network.

II.I. Energy Harvesting

Several technologies exist to extract energy from the environment, such as solar, thermal, kinetic energy, and vibration energy, and the network lifetime may increase by using power harvesting technologies. The advantages of energy harvesting systems as the ability to recharge after depletion and to monitor energy consumption, which may be required for network management algorithms. Energy harvesting technologies plays an important role in applications that are expected to operate for a long duration. There are various challenges in energy harvesting management. It classified energy sources into four categories and corresponding challenges: uncontrolled/predictable, uncontrollable, unpredictable, fully controlled and partially controllable. The energy management in energy harvesting systems is fundamentally different from battery operated systems because of the unpredictable available power. The power availability varies in time and for different nodes in the network. This presents some difficulties to a node when it has to make decisions based on knowledge of the residual energy of the network. Additionally, different nodes may have different harvesting opportunities, so it is important to assign the workload according to the energy availability at the harvesting nodes. To solve these problems, they proposed an analytical model for energy harvesting and performance. An approach to balance the harvesting energy and the load in a node. The requirement for collaboration between power management applications when the harvesting source cannot support the consumption level of the nodes load. There is a significant interest in energy harvesting for different wireless sensor applications to improve their sustainable lifetimes, but there is also a balanced need to guarantee performance and exploit the available energy efficiently. Most of the studies in the field of wireless sensors are based on residual battery status, while in harvesting systems the problem still is the estimation of the environmental energy availability at nodes. An environmental energy availability method for power management, their method is based on a predictable energy resource and cannot be used with an unpredictable resource.

III. Attack Model in WSN:

In the attack model, the attacks that are used for evaluating the performance of LB-IDS. The attacks are described with respect to each layer such as physical layer, MAC layer, and network layer.

III.A. Attack at the Physical Layer.

At the physical layer, jamming a network is a common security problem where a malicious node continuously transmits short range signals. These signal transmission create traffic in the network. Due to this traffic, a genuine node remains busy in receiving the unnecessary signals and denies other application

III.B. Attack at the MAC Layer.

At the MAC layer, getting a channel priority is a major factor. Therefore, we have considered back-off manipulation attack where the malicious node attacks the system by modifying the back off time. Here, back-off time is random in nature. It is manipulated by lowering the back-off time, so that the priority of getting the channel access increases. This increases the number of successful transmissions (Nst). In this layer, back-off time (BT) parameter and the number of successful message transmission (Nst) parameter are considered as i to detect the malicious nodes in the network. Figure 4 shows the back-off time manipulation attack where the malicious node k sends continuous signal to the genuine node j by getting the channel priority in less time.

III.C. Attack at the Network Layer.

At the network layer, routing information is mainly affected by the attackers by advertising incorrect information in the network like the minimum hop count. In this work, we have considered the sinkhole attack. In this attack, the malicious node send regular updates by advertising bogus routing information like low hop count. From Figure 5, it is observed that the malicious node 2 advertises minimum hop count to the destination (to the source node 1). The node 1 then forwards

the data in the direction of node 2. The data may be selectively forwarded to the next node or all packets are dropped. We assume that the node advertises the low hop count information in the route reply packet (RREP) during route discovery in Ad hoc On Demand Distance Vector routing protocol (AODV). Therefore, the sinkhole attack needs to be detected. In this layer, hop count (hp) parameter is considered as i to detect the malicious nodes in the network.

III.D. Cross-Layer Attack.

In cross-layer attack, a malicious node in the network attacks two or more layers at a time. In this model, we have considered the back-off manipulation attack and sinkhole attack at the MAC layer and network layer, respectively. the attacker gets high priority of accessing the channel and advertises minimum hop count information. This attack should also be detected by the LB-IDS.

IV. Sinkhole Attack, Blackhole Attack, and Grayhole Attack

WSN are majorly prone to the following packet dropping attacks: sinkhole attack, black hole attack, and gray hole attack.

IV.A. Sinkhole Attack

In sinkhole attack, the compromised node advertises itself to possess an excellent link to the base station which misleads the neighbours of the compromised node to choose and utilize the route to reach the destination node repeatedly. To attract the surrounding network traffic and to make it appear possessing an excellent link to the base station, the compromised node modifies routing packets to advertise fake routing information. Likewise, neighbors of the compromised node select forged route for data communication. In Fig. 1, the compromised node broadcasts fake route information to possess an excellent link to the base station and mislead its neighbors to forward the packets through sinkhole node to the base station. Every neighbour of the sinkhole node chooses this node to forward the data packets to the base station. In this fashion sinkhole node attracts its neighbour's node traffic. It can drop the data packets, selectively drop the data packets and tamper the data packets.

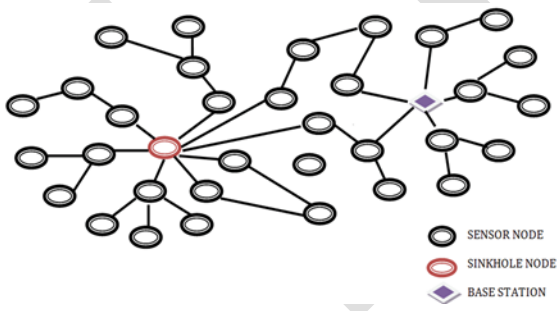

Fig. *Sinkhole attack in WSN.*

IV.B. Blackhole and Grayhole Attack

In blackhole and grayhole attack, the source node broadcast a route request to find the path to the destination node. The compromised node sends fake route information with highest sequence number and lowest hop count for the destination node when it receives route request from the source node. After receiving all the route replies, the source node approves forged malicious route since its hop count is minimum compared to the other available route. After route selection, the victim node uses the forged route to send the data. During data dissemination, the compromised node may drop all the data packets in case of black hole attack where as in gray hole attack compromised node drops the data packet statistically following a predetermined probability distribution. The primary objectives of these attacks are to attract the network traffic with fake routing information and to disturb the normal network flow.

IV.CONCLUSION

This paper deals with all common aspects of energy consumption in all types of wsn and malicious attack. Designing wireless sensor networks will enable designers to balance the energy dissipation and optimise the energy consumption among all network constituents and sustain the network lifetime for the intended application.

REFERENCES

[1] J. Sebastian Terence and Geethanjali Purushothaman "A Novel Technique to Detect Malicious Packet Dropping Attacks in Wireless Sensor Networks", J Inf Process Syst, Vol.15, No.1, pp. 203~216, February 2019.

[2] K. S. Adu-Manu, N. Adam, C. Tapparello, H. Ayatollahi, and W. Heinzelman, "Energy-harvesting wireless sensor networks (EH-WSNs): a review," ACM Transactions on Sensor Networks (TOSN), vol. 14, no. 2, p. 10, 2018.

[3] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella,"Energy conservation in wireless sensor networks: a survey," AdHoc Networks, vol. 7, no. 3, pp. 537–568, 2009.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci , "Wireless sensor networks: a survey," Computer Networks, vol.38, no. 4, pp. 393–422, 2002.

[5] S. Soro and W. B. Heinzelman, "Cluster head election techniques for coverage preservation in wireless sensor networks," Ad Hoc Networks, vol. 7, no. 5, pp. 955–972, 2009.

[6] C. Wang, J. Li, Y. Yang, and F. Ye, "Combining solar energy harvesting with wireless charging for hybrid wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 17, no.3, pp. 560–576, 2017

[7] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Detection and mitigation of sinkhole attacks in wireless sensor networks," Journal of Computer and System Sciences, vol. 80, no. 3, pp. 644-653, 2014.

[8] M. Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," Computer Communications, vol. 34, no. 1, pp. 107-117, 2011.

[9] R. W. Anwar, M. Bakhtiari, A. Zainal, and K. N. Qureshi, "Wireless sensor network performance analysis and effect of blackhole and sinkhole attacks," Jurnal Teknologi (Science & Engineering), vol. 78, no. 4-3, pp. 75-81,2016.

[10] J.Hester, T. Scott, and J. Sorber, "Ekho: realistic and repeatable experimentation for tiny energy-harvesting sensors," in Proceedings of the 12th ACM Conference on Embedded Networked Sensor Systems (SenSys '14), pp. 1–15, New York, NY, USA, November 2014.