International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-5, May 2015

A Novel Study on Data Flow Routing with Energy Optimization under Different Attacks in WSN

Leena Rani, Er. Veena Rani

***Abstract*— Designing energy-efficient and fault tolerant routing protocols for Wireless Sensor Networks (WSNs) applications is a great challenge due to the frequent change of the network topology. Moreover sensor nodes are prone to failure in WSNs due to insensitive environment. Therefore, fault tolerant and energy-efficient are major issues for WSNs. So, this paper proposes a data routing with energy optimization under different attacks in WSN. In this, it describes the attacks scenario under without cluster approach with random nodes. Then it explains the cluster based approach and also different cluster head selection for energy optimization. SO, the main objective is to handle various attacks and a dynamic routing with energy optimization. All simulations will be done in simulation tool.**

***Index Terms*— energy optimization, various attacks in WSN, data routing, Wireless sensor networks etc.**

I. INTRODUCTION

Wireless Sensor Networks have seen tremendous advantages and utilization in the past two decades. These sensors with each other to sense some physical phenomenon and then information gathered is processed to get relevant results. They consist of protocols and algorithms with self organizing capabilities. Wireless sensor networks mainly use broadcast communication while Ad-hoc networks use point to point communication. Unlike Ad-hoc wireless sensor networks are limited by sensors limited power, energy and computational capability. Sensor nodes may not have Global ID because of large amount of overhead and large no. of sensors [1].

The applications of Wireless Sensor Networks can be divided in three categories: (a) monitoring of objects (b) monitoring of an area (c) monitoring of both area and objects. Monitoring of an object consists of Structural Monitoring, ECO Physiology, Condition based maintenance, Medical diagnostics etc. Monitoring area consists of Environmental and Habitat monitoring, precision agriculture, Indoor climate control, Military surveillance, Treaty verification, intelligent alarms etc. and combination of both consist of Wildlife habitats, Disaster management, Emergency response, Asset tracking, health care etc [2]. Characteristics of WSNs mainly consists of low power, limited memory, energy constrained due to their small size. They can also be deployed in extreme environmental conditions and may be prone to animal attacks.

Leena Rani, Research Scholar, Electronics & Communication Engg. Department, JCDM Collage of Engg. Sirsa Haryana.

Er. Veena Rani, Assistant professor, Electronics & Communication Engg. Department, JCDM Collage of Engg. Sirsa Haryana.

Figure 1: Example of WSN Networks [1]

Although deployed in an Ad-hoc manner they need to be self-organized & self-healing and can face constant reconfiguration [3].

Routing protocols have a large scope of research work when implemented in a WSN, because the functions of these protocols depend upon the type of network structure designed for the application or the network operations carried out using these protocols for a specific application model [4]. Routing protocols are divided into structure based routing protocols which are in turn classified as Flat routing, Hierarchical routing, Location-based routing. (a) In Flat Routing technique all the sensor nodes play the same role such as collecting and communicating with the sink i.e. all the data collected in the remote area can be same or duplicated as all the sensor nodes work in the same way (b) Hierarchical Routing occurs with all the routing sensors in the network are clustered & a cluster head collects and aggregates the data & checks for redundancy of the data that is collected before it is sent to the sink (c) Location-base Routing consists of sensor nodes which are addressed by using their locations. Depending upon the strength of the incoming signals, it is possible to calculate the nearest neighbouring node's distance. In WSNs the only source of life for the nodes is the battery [5].
WSN. Section IV describes various routing protocols in WSN. Section V describes the proposed system. Finally conclusion is explained in section VI.

II. LITERATURE REVIEW

In Literature, author studied the Existing Fault Recovery approaches for WSN vary in forms of architecture, protocols, detection algorithm and detection decision fusion algorithm. They Provided Energy Efficient and Fault Tolerant Routing LEACH which is a modified version of the well known LEACH Protocol. EF-LEACH provides vital solutions to some shortcomings of the pure LEACH .It provide network fault tolerant and achieves reliability and quality of service.

Basically WSN faces resource constraints, high failure rates and fault caused by wireless channel and wireless sensor nodes. When a node gets failure it immediately applies its backup paths as the main path for data delivery of next incoming packets. This protocol reduces the number of dropped data packets and increases robustness of the entire network by maintaining the data packet transmission even in presence of faults [6].

Some authors proposed that topology control in a sensor network balances load on sensor nodes & increases network scalability and life time. It is envisioned that sensor nodes will be on the cubic millimetre scale, posing stringent constraints on the processing communication and storage capabilities of sensor nodes. While it is important to continue perusing novel algorithm and protocols to squeeze the most out of the existing design space, it is equally important to explore a new design paradigms for future [7].

Some proposed that multi-radio wireless mesh networks and investigate the impact when multiple wireless mesh network overlap in service area. We first find that in a system with multiple wireless mesh networks in overlap, individual mesh networks could suffer from capacity degradation if no form of inter-domain coordination is present. Therefore it is desirable to "internetwork" these wireless mesh networks by allowing inter-domain traffic relay through provisioning of "bridge" [8].

The nodes or sensing activities consumes a lot of energy in processing data & transmitting the collected data to the sink. The protocols which fall under these categories work with respect to the design constraints given for the network structure or area in sensor network [9].

Some proposed that to reduce power consumption utilizing duty cycling, sensor nodes switching to sleeping mode for most of the time is commonly used in WSN. However sensor nodes may not be able to stay awake simultaneously to communicate with each other.

Some proposed that a large scale wireless mesh networks typically has high value of network average path length which results in reduced throughput and increased delay in the network. A Load-Aware non persistent small world long link routing algorithm for small world wireless mesh networks to achieve lower average transmission path length for data transfer sessions among a set of source node and destination source node in the network. LNPR provides 58% to 95% improvement in call blocking probability and 23% to 70% in maximum load reduction [10].

Some proposed that this network signifies the need to protect sensory resources against all such attacks. Distributed load exhaustion are such attacks that may be launched by the adversarial class from multiple ends of a wireless sensor networks. The intention of such attacks is the exhaustion of victim's limited energy resources [11].

III. VARIOUS ATTACKS IN WSN

A. Misdirection Attacks:

Misdirection attack can be performed in different ways:

Packets forwarded to a node close to the actual destination. This kind of misdirection attack is less intense, because packets reach to the destination but from a different route which further produces long delay thus decreasing throughput of network.

Packets forwarded to a node at a large distance from the actual destination. It's very harmful because all packets are forwarded to a node far away, preventing them to reach the destination so packets will not reach destination.

Intermediate node becomes selfish node. Here a node in the transmission path will behave selfishly and not forward the massage packet to the actual destination. Thus here also the delay will be higher and throughput will be decrease.

If packets forwarded to a node close to the destination then Predicted delay= Normal delay + Change in delay, Throughput predicted= normal throughput- Change in throughput [12].

B. Transport Layer Attacks:

Transport layer susceptible to Flooding. Flooding can be as simple as sending many connection requests to a susceptible nodes. Prevention: Resources must be allocated to handle the connection request. Eventually a node resources will be exhausted thus rendering the node useless.

C. Black hole/Sink hole Attack:

Malicious nodes act as a black hole to attract all the traffic in the sensor network. Attackers listen to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Inserts itself between the communicating nodes it is able to do anything with the packets passing between them.

D. Hello Flooding Attack:

It uses Hello packets as a weapon to convince the sensors in WSN. Attackers with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes. Sensors are thus persuaded that the adversary in their neighbour. Victim nodes try to go through the attacker.

E. Wormhole Attack:

Attacker records the packets or bits at one location in the network and tunnels those to another location. The tunnelling or retransmitting of bits could be done selectively. Attack does not require comprising a sensor in the network rather it could be performed even at the initial.

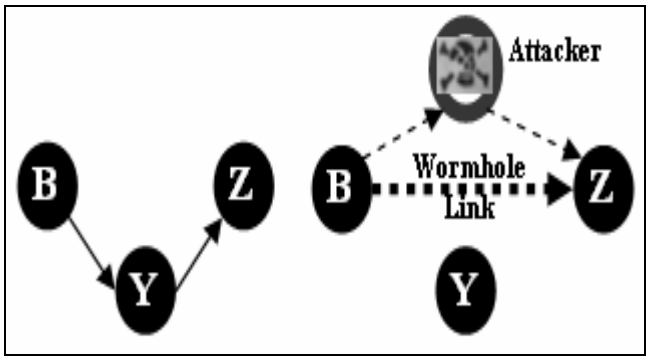

Figure 2: Wormhole Attack [12]

F. Traffic analysis attack & rate monitoring attack

For an adversary to effectively render the network useless the attacker can simply disable the base station. Rate monitoring attack makes use of the idea that node closest to the base station tend to forward more. An attacker need only monitor which nodes are sending packets and follow those nodes that are sending the most packets.

G. Time correlation Attack

Adversary generates events and monitors to whom a node sends its packets. To generate an event the adversary could simply generate a physical event that would be monitored by the sensors in the area.

H. Node Replication Attack:

Attackers seek to add a node to an existing sensor network by copying the node ID of an existing sensor node. Packets can be corrupted or even misrouted.

I. Physical Attacks:

Sensor networks typically operate in hostile outdoor environments. The small form factor of the sensors both of these together with the unattended and distributed nature of their deployment make highly susceptible to physical attacks. The current interest in wireless sensor networks has led to emergence of many application oriented protocols of which LEACH is the most aspiring and widely used protocol. On the other hand, SPIN, AODV are also some main essential protocols for WSNs in node base or cluster base approaches respectively.

IV. VARIOUS ROUTING PROTOCOLS IN SYSTEM

1. LEACH (Low Energy Adaptive Clustering Hierarchical)

We have stated that wireless sensors sense data, aggregate and then send to the base station from a remote area using the radio transmission scheme as communication system. The data which is collected by the sensors are sent to the base station, during this a lot of problematic issues such as data collision and the data aggregation. LEACH is well suited to reduce the aggregation issues by using a local data fusion which performs a compression of the amount of data that is collected by a cluster head before it sends it to the base station. All sensors form a self organized network by sharing the role of cluster head at least once [13].

The operations that are carried out in the LEACH Protocol are divided into two stages (a) The Setup Phase and (b) The Steady- State phase. In Setup Phase, all the sensor nodes within a network group themselves into some cluster regions by communicating with each other through short messages. At a point of time one sensor node acts as a cluster head and sends short messages within the network to all the other remaining sensors. A TDMA schedule is applied to all the members of the cluster group to send messages to the cluster head and then to the cluster head towards the base station. The phases using multi-hop, also direct transmission. As soon as a cluster head is selected for a region, all the cluster head of that region send the collected or sensed data in their allotted TDMA slots to the cluster head. The cluster head transmits this data in compressed format to the base station to complete the second phase which is called Steady-State Phase [14].

2. AODV (Ad-hoc On Demand Distance Vector)

AODV is a packet routing protocol designed for use in mobile Ad-hoc networks (MANET). One of a class of demand driven protocols (the route discovery mechanism is invoked only if a route to a destination is not known). Source, destination and next hop are addressed using IP addressing. Each node maintains a routing table that contains information about reaching destination nodes (each entry is keyed to destination nodes). Message types in AODV Protocols are RREQ, RREP, RRER, HELLO Messages (RREP with TTL = 1). A RREQ Messages is broadcasted when a node needs to discover a route to a destination. As a RREQ propagates through a network, intermediate nodes use to update their routing tables [15].

When a RREQ reaches to a destination node, the destination route is made available by unica sting a RREP back to the source node. A node generates a RREP if it is itself the destination. It has an active route to the destination. As the RREP propagates back to the source node, intermediate nodes update there routing tables. HELLO messages = RREP with TTL = 1. This message is used for broadcasting connectivity information. A node should use Hello messages only if it is a part of Active Route.

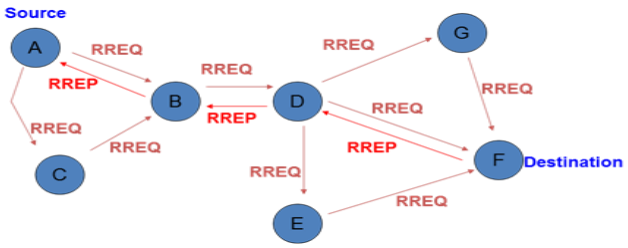

Figure 3: Message Routing in AODV [15]

V. PROPOSED ROUTING APPROACH WITH ENERGY OPTIMIZATION

Probabilistic and Non-Probabilistic Clustering Approaches contains various types of clustering protocols and their hierarchy schemes. Probabilistic approaches consist of LEACH (which we have explained earlier), HEED (Hybrid Energy Efficient Distributed Clustering), EEHC (Energy Efficient Hierarchy Clustering): HEED is an efficient and popular protocol. HEED is hierarchical, distributive, clustering technique in which single hope communication pattern is retained within each cluster, whereas multi-hop communication is allowed among base stations and clustering heads. Unlike LEACH, in HEED clustering head nodes are not selected randomly. Only sensors that have high residual energy are expected to become cluster head nodes. Also the probability to have two nodes within the transmission range of each other becoming cluster heads is small. In HEED each node is mapped exactly one cluster and can directly communicate with its cluster head.

The main objective of EEHC was to address the shortcoming of one hop common selection algorithm such as LEACH by extended the cluster architecture for multiple hops. It is a distributed k-hop clustering algorithm aiming at the maximization of the network lifetime. Initially each sensor node is elected as a cluster head with probability ‘p’ and announces its election to the neighbouring nodes within its communicating range. The above cluster heads are called “volunteer” cluster head. Next al the nodes that are within ‘k-hops’ distance from a “volunteer” cluster heads are supposed to receive the election message either directly or through intermediate forwarding. The energy consumption for network operation clearly depends upon the parameters ‘p’ and ‘k’ of the algorithm.

Non-Probabilistic Clustering Approaches: (a) Node proximity and graph based clustering protocols (b)weight based clustering protocols (c) Biologically inspired clustering approaches. Node proximity and graph based clustering protocols is a distributed multi-hop hierarchical clustering algorithm which also efficiently extends to form a

multilevel cluster hierarchy. The algorithm proceeds in two phases: Tree discovery and Cluster formation. Weight based clustering approach consists of each sensor calculates its weight after locating the neighbouring nodes in its area. The weight is a function of the sensors residual energy and the proximity to the neighbours. The node with largest weight would be elected as a cluster head and remaining nodes become members.

Biologically inspired clustering approaches attains that when two objects meet together they recognize whether they belong to the same group by exchanging and comparing information about them. In the case of WSN, initially the sensor nodes with more residual energy become cluster heads independently. Then randomly chosen nodes meet each other, exchange information and clusters are created, merged and discarded through these local meetings and comparison of their information.

A. Parameters of System

1. Number of clusters

In most recent probabilistic and randomized clustering algorithms the cluster head election and formation process lead naturally to variable number of clusters.

2. Intra-cluster communication.

In some initial clustering approaches the communication between a sensor and its designated cluster head is assumed to be direct. However multi-hop intra-cluster communication is often required.

3. Nodes and Cluster Heads Mobility

If we assume stationary sensor nodes and stationary cluster heads we are normally led to stable clusters with facilitated intra-cluster and intra-cluster management.

4. Nodes Types and Roles

In some proposed network models, the cluster heads are assumed to be equipped with significantly more computation and communication resources than others.

5. Cluster Formation Methodology

When cluster heads are just regular sensor nodes and time efficiency is a primary design criterion, clustering is being performed in a distributed manner without coordination.

6. Cluster Head Selection

The leader nodes of the cluster in some proposed algorithms can be pre-assigned. In most case however the cluster heads are picked from the deployed set of nodes either in a probabilistic or completely random way.

7. Algorithm Complexity

The fast termination of the executed protocols is one of the primary design goals. Thus the time complexity and convergence rate of most cluster formation procedures proposed nowadays is constant.

8. Overlapping

Several protocols give also high importance on the concept of node overlapping within different clusters.

9. General Approaches

To Energy Saving. We identify two main enabling techniques that are duty cycling and data driven approaches. Duty cycling is mainly focussed on signal subsystems. And data driven approaches for better efficiency. TDMA based MAC Protocols are mainly based on carrier sense multiple access which require no coordination among the nodes accessing in the channel.

10. Throughput

The amount of energy packets delivered at base station is considered in throughput value and to overcome al type of faults we use cluster base approach.

VI. CONCLUSION

Wireless sensor network are composed of many wireless sensing devices called sensor nodes. These nodes are small in size, limited in resources and randomly deployed in harsh environment. Therefore, it is not common for sensor networks to have malfunction behaviour, node, and link or network failure. In this paper, we have explained about the problem of network dis-connectivity due to cluster head failures in wireless sensor networks and we have tried to find a solution for that. We have proposed an energy-efficient, fault tolerant energy optimized protocol for wireless sensor network to diagnose faults and perform appropriate measures to recover sensor network from failures. It maintains the connectivity of the network and the reliability of data transfer even when a node in the network runs out of energy.

REFERENCES

[1] N.Gaur, A. Chakraborty and B.S. Manoj,"Load Aware Routing for Non Persistant Small World Wireless Mesh Networks" 978-1-4799-2361-8/14/$31.00 2014 IEEE.

[2] Madhu B.M., Abhilash C B,"Implementation of Improved Robust Energy Efficient Routing Protocol" 978-1-4799-6629-5/14/$31.00 2014 IEEE.

[3] Roberto D Pietro, Gabriele Oligeri, Claudio Soriente, Gene Tsudik,"United We Stand: Intrusion Resilience in Mobile Unattended WSNs"IEEE TRANSACTIONS ON MOBILE COMPUTING ,VOL. 12, NO.7,JULY 2013 .

[4] Pinaki Sarkar, Sarbajeet Mukharji,"Source Connected Scalable Combinational KPS in WSN: Deterministic Merging, Localization" 978-1-4799-0537-9/13/$31.00 2013 IEEE.

[5] Basel Alomair, Andrew Clark, Jorge Cuellar, Radha Poovendran "Toward A Statistical Framework For Source Anonymity in Sensor Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 2,FEBRUARY 2013 .

[6] Junfeng Xiao,Rose Quingyang Hu,Yi Qian,Lei Gong,BO Wang" Expanding LTE Network Spectrum With Cognitive Radios: From Concept of Implementation" 1536-1284/13/$25.00 APRIL 2013 IEEE.

[7] P. Chanak, Indrajit Banergee, Hafizur Rahaman,"Distributed Multipath Fault Tolerance Routing Scheme of Wireless Sensor Network" 978-0-7695-4941-5/13 $26.00 2013 IEEE.

[8] Messaoud Doudou, Djamel Djenouri, Nadjib Badache,"Survey on Latancy Issue of Asynchronous MAC Protocols in Delay Sensitive WSN" IEEE COMMUNICATION SURVEYS & TUTORIALS VOL.15,NO.2,SECOND QUARTER 2013 .

[9] Chih-Min Chao, Lin- Fei Lien, Chien-Yu Hsu,"Rendezvous Enhancement in Arbitrary-Duty-Cycled WSN" IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS VOL.12,NO.8 AUGUST 2013 .

[10] V.Gabale, B.Raman, P.Dutta, S.Kalyanraman,"A Classification Framework For Scheduling Algorithms in Wireless Mesh Networks"IEEE COMMUNICATIONS SURVEYS & TUTORIALS,VOL.15, NO.1FIRST QUARTER 2013 .

[11] Wei Liu, Hiroki Nishiyama,Nei Kato, Yoshitaka Shimizu, Tomoaki Kumagai,"A Novel Gateway Selection Method to Maximize the System Throughput of Wireless Mesh Network Deployed in Disaster Areas" 978-1-4673-2569-1/12/$31.00 2012 IEEE.

[12] ZHAO Jun, CHEN Xiang-guang, Xie Ying-xin,"The Application of Multipath Fault Tolerant Algorithm in WSN Codes" 978-1-4577-0536-6/11/$26.00 2011 IEEE.

[13] Chi Lin, Guowei Wu, Mingchu Li, Xiaojie Chen, Zuosong Liu, Lin Yao,"A Selfish node Preventive Real Time Fault Tolerant Routing Protocol For WSNs" 978-0-7695-4580-6/11 $26.00 2011 IEEE.

[14] P.Ghosh, Michael Mayo, V. Chaitankar, T. Habib, Ed Perkins, Sajal K Das,"Principles of Genomic Robustness Inspire Fault Tolerant WSN Topologies: A Network Science Base Case Study" SEVENTH IEEE INTERNATIONAL WORKSHOP ON SENSOR NETWOKS & SYSTEMS for PERVASIVE COMPUTING 2011 IEEE.