Performance Improvement of QoS Routing In WSN System

Kaksha Thakare[1], R.D.Patane[2]

[1]STUDENT, M.E (ELECTRONICS AND TELECOMMUNICATION)
[2]PROFESSOR, TERNA ENGINEERING COLLEGE, NERUL, NAVI MUMBAI

Email: -[1]jagdishsonawane79@gmail.com,[2]rrpatane@yahoo.co.in

Abstract- Due to the restricted communication range and high density of sensor nodes, packet forwarding in sensor networks is usually performed through multi-hop data transmission. Therefore, routing in wireless sensor networks has been considered an important field of research over the past decade. Nowadays, multipath routing approach is widely used in wireless sensor networks to improve network performance through efficient utilization of available network resources.
The field of wireless networking emerges from the integration of personal computing, cellular technology, and the Internet. This is due to the increasing interactions between communication and computing, which is changing information access from "anytime anywhere" into "all the time, everywhere". With the increased application of wireless sensor networks (WSNs) to military and civilian environments, securing the data in the network has become a critical issue. The severe resource constraints of sensor nodes and the broadcast nature of the wireless links as well as the challenging deployment environments of wireless sensor networks pose challenges for the quality and security of data transmission for these networks. In order to ensure data security and quality of service required by an application in an energy efficient way, we propose a mechanism for QoS routing with coding and selective encryption scheme for WSNs.

Index Terms- Wireless sensor network, Quality of service , Routing techniques ,coding.

1. INTRODUCTION

Wireless sensor network (WSN) is the collection of these homogenous, self-organized nodes called sensor nodes. These nodes have the capabilities of sensing, processing and communication of data with each other wirelessly using radio frequency channel.WSNs are resource constrained distributed systems with low energy, low bandwidth and short communication range. The basic features which make WSNs different from the traditional networks are; self-organizing capabilities, short range communication, multi-hop routing, dense deployment, limitation in energy and memory, and also frequently changing topology due to fading and failures. The constrained resource nature and unpredictable network structure (sensor nodes are scattered densely in an environment) poses numerous design and communication challenges for WSNs.
All nodes in a network communicate with each other via wireless communication. Moreover, the energy required to transmit a message is about twice as great as the energy needed to receive the same message. The route of each message destined to the base station is really crucial in terms network lifetime: e.g., using short routes to the base station that contains nodes with depleted batteries may yield decreased network lifetime. Always selecting the shortest route towards the base station causes the intermediate nodes to deplete faster, this results in a decreased network lifetime & also result in lowest energy consumption and lowest network delay.
Basically, each sensor node comprises sensing, processing, transmission, mobilize, position finding system, and power units. Sensor nodes are usually scattered in a sensor field, which is an area where the sensor nodes are deployed. Sensor nodes coordinate among themselves to produce high-quality information about the physical environment. Each sensor node bases its decisions on its mission, the information it currently has, and its knowledge of its computing, communication, and energy resources. Each of these scattered sensor nodes has the capability to collect and route data either to other sensors or back to an external base station. A base-station may be a fixed node or a mobile node capable of connecting the sensor network to an existing communications infrastructure or to the Internet where a user can have access to the reported data.

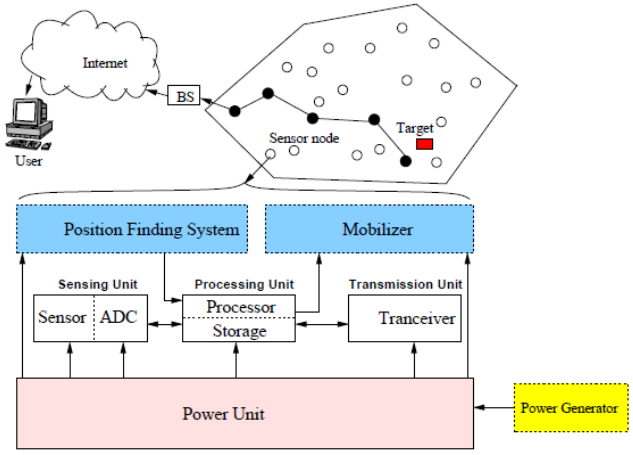

Fig 1: component of sensor node

Finally, the routing objectives are tailored by the application; e.g., real-time applications require minimal network delay, while applications performing statistical computations may require

maximized network lifetime. Hence, different routing mechanisms have been proposed for different applications. These routing mechanisms primarily differ in terms of routing objectives and routing techniques, where the techniques are mainly influenced by the network characteristics.

Resource constraints apply to both sensors and actuators, notwithstanding. In the presence of resource constraints, the network QoS may suffer from the unavailability of computing and/or communication resources. For instance, a number of nodes that want to transmit messages over the same WSAN have to compete for the limited bandwidth that the network is able to provide. As a consequence, some data transmissions will possibly experience large delays, resulting in low level of QoS. Due to the limited memory size, data packets may be dropped before the nodes successfully send them to the destination. Therefore, it is of critical importance to use the available resources in WSANs in a very efficient way. WSANs must be adaptive and flexible at runtime with respect to changes in available resources. For example, when an intermediate node dies, the network should still be able to guarantee real-time and reliable communication by exploiting appropriate protocols and algorithms.

The remaining section of the paper are as follows: In section 2 we describe routing and routing objectives in WSN, taxonomy of routing protocols and routing challenges. In section 3 QoS model of WSN and challenges support for QoS.In section 4 coding in WSN. Finally, conclusion is outlined in section 5.

2. ROUTING IN WSN

Routing is an essential problem in any type of networks. Compared with existing routing protocols, secure routing or WSNs is a very challenging task due to the severe resource constraints of sensor nodes; the broadcast nature of the wireless links makes the WSNs vulnerable to link attacks that include passive eavesdropping, active impersonation, message replay and message distortion, dynamically changing in the size and density of the network, as well as the high risk of physical attacks to sensors.

The design of routing protocols for WSNs is challenging because of several network constraints. WSNs suffer from the limitations of several network resources, for example, energy, bandwidth, central processing unit, and storage .

The performance demands of the wireless sensor networks are application specific, routing protocols should be able to satisfy the QoS demands of the application for which the network is being deployed[3].

Routing Objectives:-

Non-real time delivery: The assurance of message delivery is indispensable for all routing protocols. It means that the protocol should always find the route between the communicating nodes, if it really exists. This correctness property can be proven in a formal way, while the average-case performance can be evaluated by measuring the message delivery ratio.

Real-time delivery: Some applications require that a message must be delivered within a specified time, otherwise the message becomes useless or its information content is decreasing after the time bound. Therefore, the main objective of these protocols is to completely control the network delay. The average-case performance of these protocols can be evaluated by measuring the message delivery ratio with time constraints.

Network lifetime: This protocol objective is crucial for those networks, where the application must run on sensor nodes as long as possible. The protocols aiming this concern try to balance the energy consumption equally among nodes considering their residual energy levels. However, the metric used to determine the network lifetime is also application dependent. Most protocols assume that every node is equally important and they use the time until the first node dies as a metric, or the average energy consumption of the nodes as another metric. If nodes are not equally important, then the time until the last or high-priority nodes die can be a reasonable metric.

The Taxonomy of Routing Protocols:-

Many routing solutions that have been specifically designed for WSNs[5].These routing techniques can be classified according to the protocol operation as negotiation based, query based, QoS based, and multi-path based, as depicted in Fig. 1.

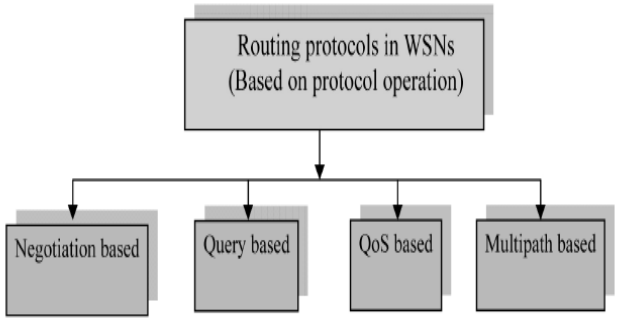

Fig 1:Classification of routing protocol based on protocol Operation

The negotiation based protocols have the objective to eliminate the redundant data by including high level data descriptors in the message exchange. In query based protocols, the sink node initiates the communication by broadcasting a query for data over the network. The multipath based protocols were initiated with objectives to provide reliability and to balance the traffic load in the network. These protocols use multipath in order to achieve better energy efficiency and network robustness in case of node failures. Multi-path routing protocols have been discussed in WSN literature for several years now.

QoS based protocols allow sensor nodes to balance between the energy consumption and certain pre-determined QoS metrics, such as delay, energy, reliability, bandwidth, etc., before they deliver the data to the sink node.

3. ROUTING CHALLENGES IN WSN

Limited energy capacity: Since sensor nodes are battery powered, they have limited energy capacity. Energy poses a big challenge for network designers in hostile environments, for example, a battlefield, where it is impossible to access the sensors and recharge their batteries. Thus, routing protocols designed for sensors should be as energy efficient as possible to extend their lifetime.

Sensor locations: Most of the proposed protocols assume that the sensors either are equipped with global positioning system (GPS)

receivers or use some localization technique to learn about their locations.

Limited hardware resources: These hardware constraints present many challenges in software development and network protocol design for sensor networks, which must consider not only the energy constraint in sensor nodes, but also the processing and storage capacities of sensor nodes.

Massive and random node deployment: In most applications, sensor nodes can be scattered randomly in an intended area or dropped massively over an inaccessible or hostile region. If the resultant distribution of nodes is not uniform, optimal clustering becomes necessary to allow connectivity and enable energy efficient network operation.

Network characteristics and unreliable environment: A sensor network usually operates in a dynamic and unreliable environment. The topology of a network changes frequently due to sensor addition, deletion, node failures, damages, or energy depletion. Also, the sensor nodes are linked by a wireless medium, which is noisy, error prone, and time varying. Therefore, routing paths should consider network topology dynamics due to limited energy and sensor mobility as well as increasing the size of the network to maintain specific application requirements in terms of coverage and connectivity.

Data Aggregation: Data aggregation technique has been used to achieve energy efficiency and data transfer optimization in a number of routing protocols.

Diverse sensing application requirements: Sensor networks have a wide range of diverse applications. No network protocol can meet the requirements of all applications. Therefore, the routing protocols should guarantee data delivery and its accuracy so that the sink can gather the required knowledge about the physical phenomenon on time.

Scalability: Routing protocols should be able to scale with the network size. Also, sensors may not necessarily have the same capabilities in terms of energy, processing, sensing, and particularly communication.

4. QoS MODEL OF WSN

A common approach to satisfy some QoS requirements in Wireless Sensor Networks (WSNs) is to use forward error correction (FEC) technique as a replication mechanism in multipath routing to increase data transmission reliability, decrease energy consumption and increase network lifetime while avoiding the costly or impossible data retransmission due to the severe resource constraints of sensor nodes . Routing is an essential problem in any type of networks. Compared with existing routing protocols, secure routing for WSNs is a very challenging task due to the severe resource constraints of sensor nodes; the broadcast nature of the wireless links makes the WSNs vulnerable to link attacks that include passive eavesdropping, active impersonation, message replay and message distortion, dynamically changing in the size and density of the network, as well as the high risk of physical attacks to sensors.

General QoS model for WSN:

In recent years, Wireless Sensor Network (WSN) has become one of the cutting edge technologies for low power wireless communication. The fast development of low power wireless communication devices, the significant development of distributed signal processing, adhoc network protocols and pervasive computing have collectively set a new vision for wireless sensor networks . In majority of WSN applications, a large number of sensor nodes are deployed to gather data based on application domains. This data collection process can be continuous, event driven and query based . Lot of research works have been done on various aspects of WSNs including protocol and architecture, routing, power conservation etc.

Quality of Service (QoS) support in WSNs is still remained as an open field of research from various perspectives. QoS is interpreted by different technical communities by different ways .In general, QoS refers to quality as perceived by the user or application. In networking community, QoS is interpreted as a measure of service quality that the network offers to the end user or application. Figure 2 shows a general QoS model for network.

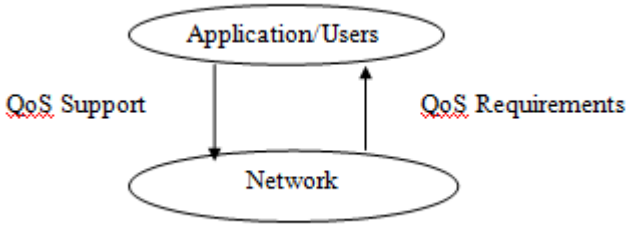

Fig 2: A Simlified QoS model

In traditional data network, QoS defines certain parameters such as packet loss, delay, jitter, bandwidth etc. However, the QoS requirements in WSNs such as data accuracy, aggregation delay, coverage, fault tolerance and network lifetime etc. are application specific and they are different from the traditional end-to-end QoS requirements due to the difference in application domains and network properties. Although some QoS solutions (like IntServ, DiffServ etc)are developed for traditional networks, these cannot be easily ported in WSNs due to

1) severe resource constraints in sensors nodes,
2) large-scale and random deployment of sensors nodes and
3) application specific and data-centric communication protocols in WSNs.

Challenges for QoS Support in WSNs :

QoS provisioning in WSN has some significant challenges. Some of such challenges are as follows.

Extreme Resource Constraint: Some of the very significant resource constraints in WSN are energy, bandwidth, buffer size and transmission capacity of the sensor nodes. Among these, efficient energy utilization of sensor nodes is a crucial issue as in most of the cases the batteries of the sensor nodes are not rechargeable or replaceable. Efficient bandwidth utilization is also a significant challenge in WSN. The traffics in WSNs can be mixture of real time and non real time. So there should be balanced allocation of bandwidth between real time and non real time traffic.

Redundant Data: Since the sensor nodes are densely deployed in a terrain of interest, therefore most of the data generated by sensor nodes are redundant. While this redundancy helps in

reliability and fault tolerance of the WSNs, it also causes a significant amount of energy wastage. Data aggregation or data fusion is a solution to remove this redundancy For example image data generated by sensors pointing to the same direction can be aggregated as those data are less variant. However, data aggregation or data fusion techniques complicate QoS design in WSNs.

Heterogeneity of the Sensor Nodes: Handling heterogeneous data generated by different types of sensor nodes is another challenge in WSNs. For instance, there are some applications which require different types of sensors to monitor temperature, pressure and humidity of the surrounding environment, capturing image or video of moving objects. Data generated from these sensors at different rates based on different QoS constraint and delivery models. Therefore, these types of diversified sensor network may impose significant challenges to provide QoS.

Dynamic Network Topology and Size: Due to mobility of sensor nodes, link failure and node failure, the topology of the network may get changed. Self reorganizing and making this network adaptable to such changes is a challenging issue in Wireless Sensor Networks. A typical WSN may consist of hundreds to thousands of densely deployed nodes in a terrain of interest. The number of such sensor nodes may increase even after the initial deployment of the network due to the newly added nodes. Though these nodes are subjected to failure, the QoS should not be affected drastically due to increase or decrease of sensor nodes.

Less Reliable Medium: The communication medium in WSN is radio. This wireless medium is inherently less reliable. The wireless links are also very much affected by different environmental factors such as noise and cross signal interference.

Mixed Data Arrival Pattern: In a typical WSN application some sensory data may be created a periodically and these are mainly due to the detection of some critical events at unpredictable times. Again there can be some sensory data which are created at a regular interval of time e.g., continuous real time monitoring of some environmental parameters. Moreover the period of periodic data may or may not be known a priori and this may depend on the kind of application. Therefore data to be handled in a typical WSN may be a mixture of periodic and a periodic type. This mix nature of data poses significant challenges in designing QoS based schemes (i.e., for guaranteeing timely and reliable delivery) for WSN.

Multiple Sinks or Base Stations: Even though most of the sensor networks have only single sink or base station, there can be multiple sink nodes depending on the application's requirements. Wireless Sensor Networks should be able to maintain diversified level of QoS support associated with multiple of sinks or base stations.

5. CODING

our{encryption technique} proposed approach encrypts only a certain fraction of Reed-Solomon codewords and the remaining portion is transmitted unprotected.. Some other encryption techniques have also been used in the area for secure multipath routing protocols.

One of them is MVMP i.e. multi- version multi-path protocol. This protocol gives the secure and reliable data communication.

MVMP consists of four steps-

1.The original data packet is divided into different groups.

2.Each group is encrypted using different cryptographic algorithms.

3. Using Reed-Solomon encrypted packets gets coded

4. Before transmitting the data packets it has been established on the multiple disjoint paths.

To transfer the data on correct path, node-disjoint path routing protocol is used. It is also used to minimize the worst case security risk and to maximize the packet delivery ratio under attacks.

In this paper, new mechanism is used that adapts to the resource constraints of WSNs by combing FEC technique and few selective cryptographic algorithms to achieve reliable and secure data transmission.

6. SYSTEM MODEL

A. Replication and erasure coding- Erasure coding has been used in distributed systems to obtain load balancing and fault tolerance. In early years it can also be used for WSNs as a replication mechanism in multipath routing to achieve reliable and secure data transmission. The advantage of data replication is to avoid the data retransmission in WSNs caused by severe resource constraints of sensor nodes which is very costly.

The one of the most simplest and widely used FEC codes is Reed-Solomon (RS)coding.

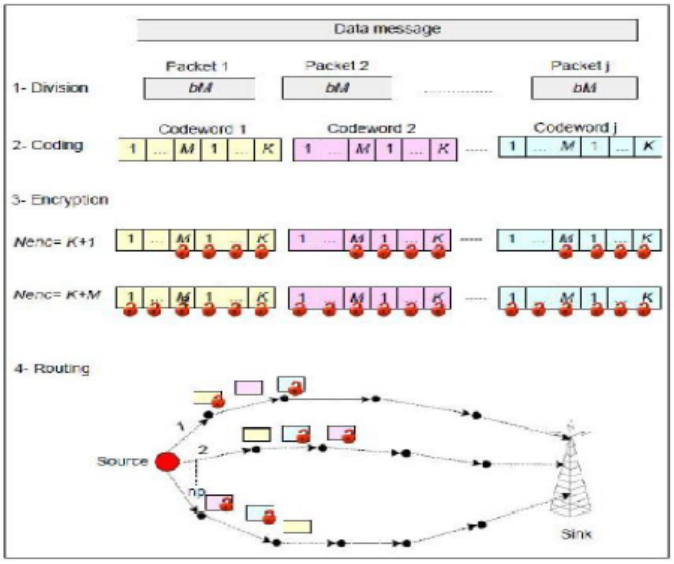

Fig 3:-The proposed mechanism

An Efficient Coded Based QoS Routing Mechanism In Wireless Sensor Networks.

B. Replication and erasure coding- Erasure coding has been used in distributed systems to obtain load balancing and fault tolerance. In early years it can also be used for WSNs as a replication mechanism in multipath routing to achieve reliable and secure data transmission. The advantage of data replication is to avoid the data retransmission in WSNs caused by severe resource constraints of sensor nodes which is very costly.

The one of the most simplest and widely used FEC codes is Reed-Solomon (RS)coding.

Reed-Solomon coding- Reed-Solomon codes are block-based error correcting codes. The Reed-Solomon encoder takes a block of digital data and adds extra "redundant" bits. Errors occur during transmission or storage for a number of reasons (for example noise or interference, scratches on a CD, etc). The Reed-Solomon decoder processes each block and attempts to correct errors and recover the original data. The number and type of errors that can be corrected depends on the characteristics of the Reed-Solomon code.

A. Multipath Routing Protocols- Data routing is an essential topic because distributed network Has many nodes and they services many messages. In short each node is a shared node since they have to make many decisions. This is very complicating. That is why routing is a very important topic in WSNs. Routing can be fixed, adaptive, centralized, distributed, etc.
The multipath routing technique which has demonstrated its efficiency to improve wireless sensor performance is efficiently used to find alternate paths between sources and sink.

Ad-hoc On-Demand Distance Vector Routing Protocol(AODV) has been used to route the data towards the appropriate node.

Ad-hoc On-Demand Distance Vector Routing Protocol- Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad hoc networks. In AODV. The network has been silent until needed connection. At that time, network node which needs the connection sends a request for connection. Other node forwards that message and records it that they heard it from. The receiver sends back the temporary route. The needy node then starts using the route which has the least number of counts. When link fails, routing error is passed back to a transmitting node and the process repeats. The main advantage of this protocol is having routes established on demand and that destination sequence numbers are applied find the latest route to the destination. The connection setup delay is lower. It uses the shortest path algorithm.

7. MATH

Figure 3 shows the steps included in this mechanism. System model involves following steps.
1 .Divide the data message into packets such as each packet is of size

$$K=bM \quad (1)$$

2. Encode the data packet by using FEC technique which includes the Reed-Solomon coding in such a way that each codeword having the set of total M+K fragments. Where M is the number of fragments and K is the number of encoded fragments.
3. Depending on the security level required, the number of fragments to be encrypted ,

$$Nenc=K+E \quad (2)$$

Where Nenc is the total number of fragments encrypted and E is determined according to the required security level and

$$1\leq E\leq M. \quad (3)$$

4. Route all the fragments on the np disjoint paths to the node and in order to enhance the security the encrypted fragments from the same codeword are transmitted on different paths.

5. At the receiving node, the encrypted fragments are first decrypted and then all the fragments are encoded to reconstruct the original data packet.

CONCLUSION

This research indicated that in order to ensure data security and quality of service required by an application in an energy efficient way, we propose a mechanism for QoS routing with coding and selective encryption scheme for WSNs. In this project, we presented a new routing mechanism, which integrates FEC codes and selective encryption scheme for providing both QoS and secure data transmission in WSN.

ACKNOWLEDGE

I gratefully acknowledge the contribution of Prof. R.D.Patane of Terna Engg. College for the support for the original version of this document.

REFERENCES

[1] S. K. Singh, M.P. Singh, and D.K. Singh, "A Survey on Network Security and Attack Defense Mechanism for Wireless Sensor Networks," International Journal of Computer Trends and Technology, Vol. 1(2), pp. 9-17, 2011.
[2] Hind Alwan, and Anjali Agarwal ,"a secure mechanism for qos routing in wireless sensor networks",2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE).
[3] Marjan Radi , Behnam Dezfouli , kamalrulni Zam Abu Barkar and Malrey Lee,"Multipath Routing in Wireless Sensor Networks: survey and research challenges",2012 sensors.
[4] A. Wood, and J. Stankovic , "AM Secure : Secure link-layer Communication in TinyOS for IEEE 802.15.4-based wireless sensor Networks," In proceedings of the fourth International Conference of Embedded Networked Sensor systems, NewYork, USA, pp. 395–396, 2006.
[5] R. Sumathi and M.G. Srinivas ,"A Surey of QoS Based Routing Protocols For Wireless Sensor Networks ,JIPS 2012.8.4.589.
[6] Shiv Kumar Singh, M. P. Singh and D. K. Singh , "Routing Protocols in Wireless Sensor Networks-A Survey," International Journal of Computer and Engineering Survey (IJCSES), Vol. 1,no.2,Nov 2010.

AUTHORS

1.KAKSHA THAKARE - M.E (Electronics and telecommunication), jagdishsonawane79@gmail.com
2. R. D. PATANE – Professor , Terna Engineering College, Nerul , Mumbai University, rrpatane@yahoo.co.in.