RESEARCH ARTICLE OPEN ACCESS

Study Of Coded Based Mechanism In WSN System

Kaksha S.Thakare*, R.D.Patane**
**(Department Of Electronics and Telecoumication, Mumbai University, India)*
*** (Department Of Electronics And Telecoumication, Mumbai University,India)*

ABSTRACT
Wireless Sensor networks (WSN) is an emerging technology and have great potential to be employed in critical situations like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios.One of the major challenges wireless sensor networks face today is QoS. 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.Our approach provides reliable and secure data transmission and can adapt to the resource constraints of WSNs.

***Keywords* -** Error Correcting code,Quality of Service,Selective encryption algorithm,Wireless Sensor Network ,etc

I. INTRODUCTION

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.

Wireless Sensor Networks(WSNs) use tiny, inexpensive sensor nodes with several distinguishing characteristics: they have very low processing power and radio ranges, permit very low energy consumption and perform limited and specific monitoring and sensing functions. Several such wireless sensors in a region self-organize and form a WSN. Information based on sensed data can be used in agriculture and livestock, driving or even in providing security at home or in public places. A key requirement from both the technological and commercial point of view is to provide adequate security capabilities. Fulfilling privacy and security requirements in an appropriate architecture for WSNs offering pervasive services is essential for user acceptance. Five key features need to be considered when developing WSN solutions: Scalability, security, reliability, self-healing and robustness. The security in wireless sensor networks (WSNs) is a critical issue due to the inherent limitations of computational capacity and power usage.

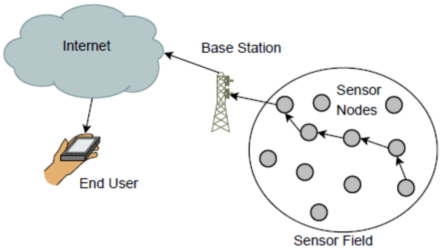


Fig 1 :- Wireless Sensor Network Model and Architecture

The following illustrate the key components of sensor networks:

Sensor Field: A sensor field is vicinity where thenodes can be positioned.

Sensor Nodes: Sensors nodes are the heart of the network. It is the responsibility of the sensor nodes to gather information and transmit to the sink or base station; it is engineered for the network.

Sink: Sink receives data from various nodes, and then process and stored all the data collected from the nodes. Message correspondences between nodes are diminished because of the sink therebydecreasing energy conditions of the entire network.

Base station: The base station also called the centralized control room for data extraction, spread information back and forth to the networks, data processing and storage center with user access controls.

Data is streamed to these workstations either via the internet, wireless channels, satellite etc.Sensor networks deployed in a specific geographical area does construct a wireless multi-hop network, and the sensor nodes apply wireless medium for transmission namely infrared, radio, Bluetooth during communication.

We will look into the challenges of QoS provisioning in WSNs and some of the existing developments in QoS mechanisms for WSNs.

1. Difficulties of QoS provisioning in WSNs

The successful deployment of QoS in WSNs is a challenging task because it depends on both the inherent properties of the network, as well as the physical hardware constraints of the sensor nodes.

2. QoS Performance Metrics in WSNs

Unlike the Internet and MANETs which can be used for a multitude of applications ranging from file transfer to multimedia applications, each WSN is usually deployed for a specific application such as environmental monitoring or target tracking. In addition, each of these networks has their own unique characteristics and constraints; consequently, the QoS performance metrics in WSNs may differ significantly from those that are used in the Internet and MANETs.

3. Mechanisms to Achieve QoS in WSNs

In this section, we describe some existing mechanisms that have been proposed in the literature, which allow WSNs to achieve QoS.

3.1 Topology Management:- To reduce the amount of energy that is consumed by a sensor node in the network, the nodes can be put to sleep mode when they are not required to sense or transmit data to their neighbouring nodes.Topology management helps to increase energy efficiency (and thus network lifetime) at the expense of higher latency, because nodes that are required for the data forwarding process may be in sleep mode during the transmission.

3.2 Localization:-Localization provides an alternative mechanism of finding the physical locations of the sensor nodes in the network instead of making use of GPS, which is costly and infeasible indoors. localization increases spatial accuracy, at the cost of higher overheads (and transmissions) which will reduce energy efficiency.

3.3 Controlled Mobility:-To incorporate QoS in the sensor network, controlled mobility using mobile nodes or Unmanned Autonomous Vehicles (UAVs) can be used to deploy sensor nodes more efficiently to enhance connectivity and/or coverage.

3.4 Data Aggregation and/or Fusion:- This helps to reduce redundancy caused by spatial correlation of the sensed data and minimize the number of transmissions required to forward the data back to the sink.

3.5 Network Topology:- This helps to improve the load distribution of the network and increases the network lifetime, at the expense of the physical deployment of more sinks.

3.6 Cross-Layer Designs:- Cross layered designs such as that proposed by Chen et al can help to improve network performance by sharing information across the different layers, at the cost of eliminating the interdependency between adjacent layers.

4. Open research issues in QoS support in WSNs.

4.1 Services: What kind of non-end-to-end services can WSNs provide?Are traditional best effort, guaranteed, and differentiated services still feasible in this new paradigm?

4.2 QoS support based on collective QoS parameters: It is very interesting to explore the support mechanisms for three classes of data delivery models using collective QoS parameters. Further, how do the mechanisms differ from those in traditional networks?

4.3 Traditional end-to-end energy-aware QoS support: Al- though these are not of main concern in WSNs, they may be applied in some scenarios. Also, it is very interesting to explore the limit on QoS assurance in an extremely resource- constrained network.

4.4 Trade-offs: Data redundancy in WSNs can be intrinsically exploited to improve information reliability. However, it spends too much energy to transmit these redundant data. If we introduce data fusion, it can reduce data redundancy in order to save energy, but it also introduces much delay into the network. What is an optimum trade-off among them? This optimum trade-off may be achieved analytically or by network simulations.

4.5 Adaptive QoS assurance algorithms: It is desirable to maintain QoS throughout the network life instead of having a gradual decay of quality as time progresses. This prevents gaps in data sets received by the sink. These gaps, that directly affect QoS, are caused by network dynamics. As a result, some adaptive QoS algorithms may be required to defend against network dynamics.

4.6 Service differentiation: What is the criteria of differentia- tion? Should it be based on traffic types, data delivery models, sensor types, application types, or the content of packets? Considering the memory and processing capability limitations, we cannot afford to maintain too many flow states in a node. Thus, it is desirable to control network resource allocation to a few differentiated traffic classes such that a desired maximum resource utilization is obtained.

4.7 QoS support via a middleware layer: If QoS requirements from an application are not feasible in the network, the middleware may negotiate a new quality of service with both the application and the network. Such a middleware layer, which may be used to translate and control QoS between the applications and the networks, is of great interest.

4.8 QoS control mechanisms: Sensors may send excessive data sometimes and thereby waste precious energy while they may also send inadequate data at other times so that the quality of the application cannot be met. Some novel centralized or distributed QoS control algorithms are desired.

4.9 The integration of QoS support: The mechanisms of QoS support in WSNs may be very different from that in traditional networks. However, since the requests to WSNs can be from a User/application through a traditional network such as the Internet, further research is necessary for handling the differences between them and maintain the QoS services seamless to the application running over both networks.

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. Traditional encryption techniques are too complex and also it introduces some severe delay in sensor nodes. The two basic methods to recover erroneous packets in any network are Automatic Repeat Request (ARQ), and Forward Error Correction (FEC). The life time of any wireless sensor network depends directly on the efficient use of its power resources. Power is primarily consumed during wireless transmission and reception. As energy conservation is a major issue of concern in WSN, repeat transmission is not an option and FEC would be preferred over ARQ.

II. FORWARD ERROR CORRECTION

The main design concern for any applications of wireless sensor networks is the limited energy supply,limited computation capability and communication range of sensor nodes as compared with other computing and communicating devices The nodes play a dual role as data sender and data router in a multi-hopWSN. Aggressive energy management techniques are used to fulfill the main design goals of WSNs which is to carry out data communication while trying to prolong the lifetime of the network and prevent connectivity degradation. One way to conserve the energy in WSNs is to avoid retransmission due to error as far as possible and instead use efficient error control scheme for error correction.

Forward error correction (FEC) also called channel coding is a system of error control for data transmission, whereby the sender adds systematically generated redundant data to its messages, also known as an error-correcting code.FEC gives the receiver an ability to correct errors without needing a reverse channel to request retransmission of data, but this advantage is at the cost of a fixed higher forward channel bandwidth.FEC is therefore applied in situations where retransmissions are relatively costly, or impossible such as when broadcasting to multiple receivers.

In particular, FEC information is usually added to mass storage devices to enable recovery of corrupted data. The maximum fractions of errors or of missing bits that can be corrected are determined by the design of the FEC code, so different forward error correcting codes are suitable for different conditions.

In FEC source node encodes data using some error correcting code which lets the receiver node to correct errors in data packet if present, thus making retransmission outdated.Error control coding also provides coding gain which lowers required transmitting power for specific bit error rate (BER) or frame error rate (FER).

However this happens at cost of extra energy consumption in encoding, transmitting redundant bits and decoding. In most cases encoding energy is considered to be negligible while decoding process consumes significant amount of energy.Complex decoders provide better performance in term of BER but on the other hand consume more energy[6].

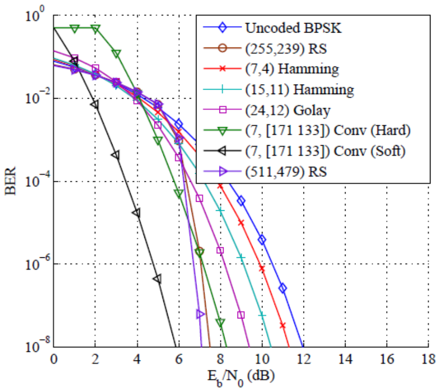


Fig 2:-BER analysis for different error correcting codes

WSNs are energy constraint and also require reliable data communication, so the data reliability must be provided at low energy cost.Hence it is very challenging to choose an optimum error correcting code for wireless sensor network where both, the performance and energy consumption are taken into account.

Someresearchers have studied hybrid automatic repeat request (HARQ) schemes which exploit advantages of both error correcting schemes by combining ARQ and FEC. HARQ is good for some scenarios in wireless sensor networks but it is limited to only specific applications and consumes a significant amount of energy.

Error correcting codes insert parity bits into message sequence in a proper way depending on type of code being used. The parity bits allow the receiver to correct errors in message sequence if introduced due to noise or interference during transmission. The system with error control coding provides better BER performance as compared to un-coded system for same SNR[5].

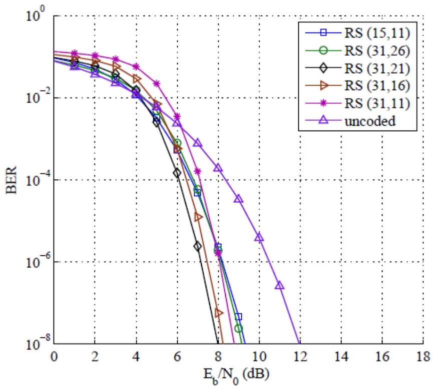


Fig 3:-BER analysis for different Reed Solomon codes

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.

III. SELECTIVE ENCRYPTION ALGORITHM

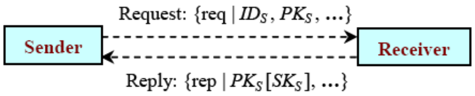
Encryption is the process of encoding plaintext into cipher text and decryption is the reverse process. Through the data encryption and decryption, the protection of data confidentiality and integrity are achieved. However, based on the features of wireless devices, a wireless ad hoc network has special security and efficiency requirements for conventional cryptographic algorithms.

Selective encryption algorithms are primarily applied in the realms of energy-aware environments or large scale data transmission such as, multimedia communications, mobile ad hoc networks (MANETs), wireless sensor networks (WSNs), etc. For multimedia communications, it often requires real-time data transmission, so tremendous audio and video data need to be transferred securely. Selective Encryption algorithm reduce computation time and power without compromising the security of the transmission.

There are three methods for Selective Encryption Algorithms[5]:

1. Secure Key Distribution(Full Encryption)

The figure.1 illustrates the procedure of secret key distribution between a pair of nodes. The message's sender composes a communicating request message req which contains not only its identifier IDs, but also its public key PKs, for the purpose of their later mutual authentication. Once the receiver gets such a communication request, a secret key (symmetric key) SKs will be generated by the receiver and encrypted using the public key PKs of the requester, which is included in the communicating request message. Later, the receiver composes a communicating reply rep message and replies it to the communicating sender, in order to indicate that their communication has been successfully established. After the sender obtains the response from the receiver, it will use its corresponding private key PRs to decrypt the secret key SKs issued from the receiver.


Request: $\{req \mid ID_S, PK_S, \ldots\}$
Sender
Receiver
Reply: $\{rep \mid PK_S[SK_S], \ldots\}$

2. A Probabilistic Selective Encryption Algorithm

Here, a probabilistically selective encryption algorithm, which uses the advantages of the probabilistic methodology, aiming to obtain sufficient uncertainty.

During the process of sending messages, the sender will randomly generate a value to indicate the encryption percentage, which represents how many messages will be encrypted among the transmitted messages.Then, the sender uses a probabilistic function to choose the already deterministic amount of messages to encrypt them.

The probabilistic selective encryption algorithm integrates both the probabilistic method and stochastic strategy, in order to increase the uncertainty in the process of message selection.

3. A Toss-A-Coin Selective Encryption Algorithm

In order to provide sufficient security to data encryption, we choose a relatively high proportion as encryption ratio. Since the toss-a coin algorithm is a basic approach, little uncertainty is involved. For all transmitted messages, we divide them to two groups: the odd number messages and the even number messages.

When the sender needs to decide which group should be encrypted, it makes use of a toss-a-coin method to determine whether the even number messages or odd number messages are encrypted.

IV. MATH

The math include steps[8]:-

1. Divide the data message into packets such as each packet is of size

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

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 ,

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

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

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

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.

V. SIMULATION

Simulation by using MATLAB software will give exact brief idea about this routing mechanism. Here consider the MATLAB simulation results. Consider there are total number of 50 nodes which establishes during communication within 100msecs.Suppose the data is transmitted from node 9 to node 25. To prevent the data loss or to recover the lost data during communication due to some errors, REED- SOLOMON coding is being used.

Simulation results shows that as compared to the previous routing technique, this routing technique gives the minimum end to end delay also it maximizes the throughput such as packet delivery ratio also increases[8].

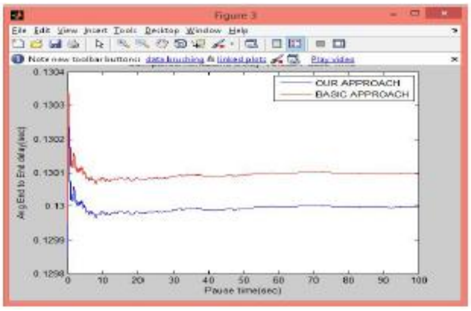


Fig 5:- End To End delay comparison

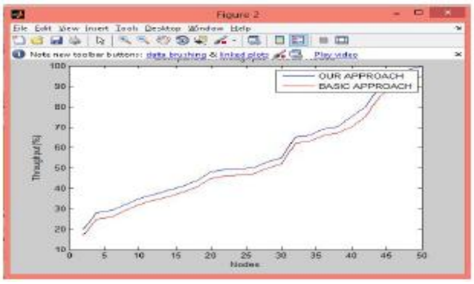


Fig 6:- Throughput comparison

VI. CONCLUSION

Wireless Sensor Network technology has an incredible potential to enhance quality of life in all aspects and is likely to be widely used in the medium-term future.To realize the full potential of this technology, there is a lot of additional work to be done in further times. Research has to focus on security aspects and higher reliability for these systems and guidelines for aspects of privacy protection have to be discussed.With these challenges in mind, the fast speed, with which further developments of the technology flood on the field, can lead to optimism and excitement on upcoming applications.

In this paper, we presented a new routing mechanism, which integrates FEC codes and selective encryption scheme for providing both QoS and secure data transmission in WSN. We will be developing the proposed technique.We will be developing the proposed technique.

ACKNOWLEDGEMENTS

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]. I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer Networks 38 (2002) 393–422

[2]. Feng Xia 1,2 ,QoS Challenges and Opportunities in Wireless Sensor/Actuator Networks, Sensors 2008, 8(2), 1099-1110, www.mdpi.org/sensors.

[3]. 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).

[4]. M.P.Singh,Prabhat Kumar, An efficient forward Error Correction Scheme for Wireless Sensor Network,Procedia Technology ,4(2012),737-742 .

[5]. Mohammad Rakibul Islam, Error Correction Codes in Wireless Sensor Network : An Energy Aware approach, International Journal of Electrical, Computer Energetic, Electronic and Communication Engineering Vol:4, No:1, 2010

[6]. Patil Ganesh, Madhumita Chatterjee, Selective

[7]. Encryption Algorithm Networks,Ad-hoc Networks

[8]. International Journal on Advanced Computer Theory and Engineering (IJACTE) ISSN (Print) : 2319 – 2526, Volume-1, Issue-1, 2012

[9]. Yonglin Ren, Azzedine Boukerche, Lynda Mokdad, Performance Analysis of a Selective Encryption Algorithm for Wireless Ad hoc Networks, IEEE WCNC 2011-Network.

[10]. Shivangi M. Salunkhe, Shashi Prabha, An Efficient Coded Based QoS Routing Mechanism in Wireless Sensor Networks, 22nd IRF, International Conference,29thMarch 2015, Chennai, India, ISBN: 978-93-82702-83-2.