Improving Reliability in Heterogeneous Wireless Sensor Networks

A.Hemalatha[1], Dr.R.Venkatesh[2]

[1,2]*Department of IT, PSNA college of engineering and Technology*
Dindigul, Tamilnadu, India

[1]hemaa9095@gmail.com

[2]rlvenkatesh@gmail.com

***Abstract*— A wireless sensor network is a type of ad-hoc network which has more challenges such as security, energy efficiency, unreliable behaviours and etc. In this paper deals about improving reliability in clustered heterogeneous wireless sensor networks. The proposed scheme explains about multipath routing for both intrusion/ fault tolerance in the presence of unreliable nodes .In our project analyses about trade off between energy consumption vs. reliability .In HWSN the nodes are grouped as a cluster in which CH aggregates the data from other sensor nodes .The multipath routing is applied to determine the redundancy level such as path redundancy and source redundancy in the presence of unreliable nodes. In this paper finds the alternate path based on the error report that report is forwarded to both source and destination node .From the set of alternate path, a reliable path will choose to transmit the data from source CH to destination node based on the path reliability and minimum hop count .The algorithm is to identify and apply the analyzed parameters at runtime to improve the network performance.**

***Keywords*—multipath routing, path reliability, unreliable node, wireless sensor networks**

I. INTRODUCTION

Wireless sensor networks are deployed in unattended areas to monitor and sense the conditions such as temperature, sound and pressure .A WSN consists of three main components: nodes, gateways and software .The gateways are used to collect the information from distributed nodes .The nodes feature as direct sensor connectivity, reliable communication in which the node is battery powered.

In wireless sensor network has more issues and challenges such as quality of service requirements, power factors, node cost and environmental factors .The trade off between energy consumption vs. reliability gain [6] to maximize the WSN network efficiency however the prior works explains about improving reliability [7] using multipath routing but it doesn't analyses about energy cost between the source and destination in the presence of unreliable nodes as a path.

Clustering is an effective solution to achieve the scalability, reliability and energy efficiency in the wireless sensor networks. Data coming from multiple sensor nodes are aggregated if they are about the same attribute of the phenomenon when they reach the same routing node on the way back to the sink. The reliability of the network depends upon three parameters such as connectivity, network parameter and data aggregation .The connectivity indicates the network connectivity, broadcast reachability of the network.

A homogeneous network [8] consists of the same types of sensors while a heterogeneous network consists of different types of sensors having different capabilities such as bandwidth ,energy requirements ,node size and etc. multipath routing is an effective mechanism to achieve reliability in the presence of unreliable node and it's to alternate the packet from error occurred path while the existing works explain about achieving reliable path and some attention has been paid to insider attacks in wireless sensor networks .The problem of reliable data transport over wireless multihop networks like wireless sensor networks is not an easy one .There are three main sources of packet losses:

- The wireless channel can introduce transmission errors, the packets of different nodes can collide, or nodes can lose packets because of other failures.
- Packets can be dropped in the network because of unreliable or unreliable node
- The receiver might drop packets because they arrive too quickly.

In this paper combines both problems as identifying multiple paths and choosing a reliable path in wireless sensor networks .For choosing a reliable path, our approach considers existing protocol parameters such as path reliability and hop count .By using these parameters the reliability of the path will be improved in heterogeneous wireless sensor networks.

The rest of the paper is organized as follows. Section II, we define our related work and section III about Proposed system. In section IV explains algorithm of the system .finally in section V analyses the simulation results .In section VI we conclude the paper and outline some future research areas.

II. RELATED WORK

Over the past years**,** several QoS provisioning Protocols have been proposed for wireless networks .However, they are based on end-to-end path finding and resource allocation, which renders their application impractical for large scale sensor networks.

Sequential assignment routing was one of the first protocols for WSN that considered QoS issues for routing decision based on three factors: energy resources, QoS planned for each path and the packet traffic type which is implemented by priority mechanism. SAR creates multipath table whose main objective is to obtain energy efficiency and fault tolerance.

SPEED [2] is another QoS routing protocol for wireless sensor network (WSN) that provides real-time end to end guarantees in sensor network. MMSPEED [3] (multipath and multi-SPEED routing Protocol) is an innovative packet delivery mechanism for QoS provisioning and focuses on timely and reliability requirements.

Our work considers heterogeneous nodes with different capabilities and different functions and also analyzes the unreliable nodes behaviors. In this paper explores the tradeoff between energy consumption vs. reliability, security to improve the network efficiency .It analyses about Multipath routing to tolerate unreliable node and also it uses geographic routing to forward the data.

The main objective of geographic routing is to use location information to formulate an efficient route search toward the destination .Our approach considers redundancy management for both fault/intrusion tolerance through Multipath routing that proposed to improve the network efficiency in wireless sensor networks.

III. PROPOSED SYSTEM

In Heterogeneous wireless sensor network [12] is a network in which some sensors having larger sensing range and more power to achieve a longer transmission. It consists of different types of sensors having different capabilities such as energy, battery power ,resources ,bandwidth and etc. we consider two types of sensors such as cluster head(CH),the source node(SN).The cluster Head having more energy when compared to the source node in which each node should have a special role in the network .The Cluster Head Plays a main role to aggregate the data from a source node .In this paper the sensor nodes are combined together to form a cluster. More than one number of clusters are combined to form a network in WSN and also clustering is used in our approach to reduce the address overhead and for energy consumption.

Generally All sensors are subject to capture attacks that attacks are classified into insider attacks and outsider attacks .Insider attacks mostly compromised the codes of the nodes in sensor network in which they are vulnerable to physical attacks [1] by the adversary nodes in which insider attacks perform eavesdropping ,stealing the information ,damage information and deny access to authorized user .Outside attacks are external to the network and that processes are committed by illegal parties .The outside attack's effects as follows in the sensor network as jamming ,triggering dos attacks and etc. In our approach [4] deals about insider attack's effects only such as node failure, transmission failure and packet dropping.

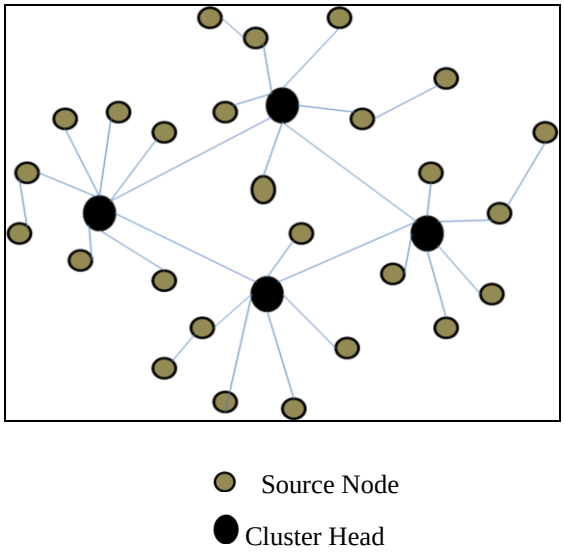

Fig. 1. Architecture of heterogeneous WSNs

We assume geographic routing protocol for WSNs is used to transfer the data between nodes in which the data aggregation can be taken place in the cluster head node .The data aggregation is used to eliminate the redundancy among packets from different sensors .Geographic routing does not maintain a heavy state at the routers to keep track of the current state of the topology .It requires only the propagation of single hop topology information such as the position of the best neighbour to forward the data.

Motivations for Using Multipath Routing Approach in Wireless Sensor Networks are Reliability and Fault-Tolerance, Load Balancing and Bandwidth Aggregation, QoS Improvement .Each sensor has a failure probability which is affected by electrical energy ,hardware failures ,communication error and undesired environment situation .There are two types redundancy: software redundancy and hardware redundancy .The hardware redundancy increases overall network consumption in which redundant nodes and redundant paths increase the fault tolerance mechanism in wireless sensor networks. The fault tolerance is the important characteristics of the network which leads the network to continue its functionality.

There are two main reasons to occur the fault in WSN. The first reason is replacing a sensor node that is hard to replace in sensor network .The second reason is low battery power in WSN. There are two strategies increases the fault tolerant factor in WSN .The path redundancy uses 'm' disjoint paths between source CH and source node .The source redundancy is done to cope with sensor or transmission faults.

A. *Initialization phase*

In heterogeneous wireless sensor network has two types of nodes such as CH (cluster Head) and SN (source Node) which are deployed in a random manner .In cluster the following action will be taken place:

- CH node broadcasts route request message and other sensor nodes receive the route request message within the coverage area.
- SN node sends route reply message to CH (cluster Head).Based on the route reply message the cluster will be formed

From Source CH (Cluster Head) to destination the CH node sends route request to other CH .Finally the requested CH receives the route reply from other Cluster head.

B. *Multipath routing*

Multipath routing [5] is to find the multiple path from source to destination. Path finding is a process of finding a path from source CH to destination. For finding a path, the following action will be taken place:

- Identifying multiple paths from source CH to the destination node
- Choosing a reliable path

C. *Checking unreliable node*

In this paper considers two ways of failure to be occurred during data transmission [9] such as

- transmission speed violation
- sensor and channel failure

An unreliable node may refuse to forward certain messages or simply drop the message in the wireless sensor network that node is isolated in network by discarding the path for data transmission .The alternate path will be chosen to forward the data based on the route reply information.

D. Packet Transmission

Reliability analysis:

It derives expressions for query reliability (R_q) and the average distance between the nodes (D_{avg}) .Let d_{sc} be a variable denoting the distance between the source CH and source node.d_{cp} be a variable denoting distance between source CH and processing center .As described in [6] the number of hops between the PC and the source CH denoted by h, is given by

$$h = \frac{d_{cp}}{r} \tag{1}$$

The average distance between the Source CH to sink is given by Eq. (2)

$$d_{cp} = \int \sqrt{(x2+y2)}\frac{1}{A} \tag{2}$$

$$d_{cp} = 0.765\frac{A}{2} \tag{3}$$

The average number of hops to forward the data from source node to processing center (PC) that is denoted as N_{cp}

$$N_{cp} = E[h] = \frac{0.3825A}{r} \tag{4}$$

The average distance between the source node to source CH is expressed in Eq. (5)

$$d_{sc} = \iint x^2 + y^2 \times \rho(x,y)dxdy = \frac{A^2}{2\prod k} \tag{5}$$

Where $\rho(x,y)$ is the node distribution and A is the area of monitoring field .The average distance between the nodes (D_{avg}) are calculated by using Eq. (6)

$$D_{avg} = \frac{1}{n}\sum_{i}^{n} Di \tag{6}$$

Where D_i is the distance between a source node and the base station.The D_{avg} can be approximated as

$$D_{avg} \cong d_{cp} + d_{sc} \tag{7}$$

The query response is transmitted from an SN to the PC through the CH hop by hop within the T_D .The query response of user request may be discarded after reaching the deadline requirement .The minimum transmission speed requirement ($S_{jk)\ is}$ given by

$$X_{set} = \frac{d_{cp} + d_{sc}}{T_D} \tag{8}$$

The values of d_{cp} and d_{sc} substituted into Eq. (9)

$$S_{jk} \Rightarrow E[x_{set}] = \frac{0.3825A + \frac{A^2}{2\prod k}}{T_D} \tag{9}$$

The transmission speed (S_{jk}) can be measured dynamically from source node to the destination node.Let $Q_{t,jk}$ be the probability of forwarding the packet from one sensor node to another node,then $Q_{t,jk}$ can be computed as

$$Q_{t,\,jk} = \frac{E[Xset]-a}{b-a} \tag{10}$$

Let $Q_{r,\,j}$ denote the probability of failure due to sensor/channel failure .since q is the hardware failure

probability as input and e_j is the transmission speed violation probability.

$$Q_{r,\ j} = 1 - [(1 - q)(1 - ej)] \quad (11)$$

By combining transmission failure violation and sensor/channel failure probabilities we can obtain $Q_{rt,jk}$ that is expressed as follows:

$$Q_{rt,\ jk} = 1 - [(1 - Q_{r,\ j})(1 - Q_{t,\ jk}) \quad (12)$$

The above expression $Q_{r,,j}$ and $Q_{t,jk}$ values are substituted. By using equation(11) we can compute probability of cluster head failing to forward the packet to one hop neighbor node that is given by,

$$\theta_j^{CH} = 1 - \prod_{k=1}^{f \times nk} Q_{rt,\ jk} \quad (13)$$

The above expression f is the fraction of neighbors that would forward the data to other nodes .The probability of single path between Source Cluster Head and processing center is expressed as follows

$$\Theta(Ncp) = (\prod_{j=1}^{Ncp-1} \theta j) \times (1 - Q_{rt,Ncp(Ncp+1)}^{CH}) \times [(1-q)(1-Q_{c,PC}^{CH})] \quad (14)$$

The probability of single path between Source Cluster Head and normal source node is expressed as follows

$$\Theta(Nsc) = (\prod_{j=1}^{Nsc-1} \theta_j^{SN}) \times (1 - Q_{rt,Nsc(Nsc+1)}^{SN}) \quad (15)$$

The failure probability of data delivery from source node to source CH that is calculated by using Eq. (15)

$$Q_{fs} = \prod_{i=1}^{m_s} [(1 - \Theta_{i(Nsc)})] \quad (16)$$

Consequently, the failure probability from source CH to processing center is also expressed same as follows

$$Q_{fp} = 1 - (1 - Q_{fp}^{m_p})(1 - Q_{fs}^{m_s}) \quad (17)$$

Therefore the query success probability is calculated by:

$$R_q = 1 - Q_{fp} \quad (18)$$

The R_q is mainly calculated to determine the reaching probability of the packet in wireless sensor networks.

In packet transmission [10], the reliable path is selected based on the path reliability and hop count.

- The path reliability is calculated for each path .If any error occurs in this path, the error report will be forwarded to both sender and destination .The error may be sensor fault, transmission fault and channel failure. We have to select a path that links should have high reliability. The path reliability expressed as

$$W_L = \prod_{i=1}^{hopcount} (1 - LERi) \quad (19)$$

Hop count and path reliability denote the number of hops and reliability of each path. LER denotes error rate of the path.

- For packet transmission the hop count should be kept low when compared to other paths in the WSN .The hop count is expressed as follows:

$$W_H = \frac{1 + \max hopcount - hopcou}{\max hopcount} \quad (20)$$

Finally the packet is transmitted from source to destination based on the reliability analysis ,path reliability and hop count.

IV. ALGORITHM

The objective of this algorithm [11] is to identify and apply the redundancy level in terms of path and source redundancy (ms, mp).Our algorithm Fig.2 and Fig.3 describes the CH execution and SN execution for managing multipath routing for intrusion tolerance to maximize the network efficiency.

All the nodes in the system updates the query periodically .we determine radio range and a transmission range of both CHs and SNs where the range is dynamically adjusted .when the mobile user issuing the queries to nearby CH .In our system there is no base station and all, the CH is acting as a base station or sink node .The issuing Queries have strict timeliness requirements such as TD timer for determining radio range, transmission range. When a CH acting as a base station receives the query from the end user, it triggers multipath routing for intrusion tolerance using the redundancy level as path redundancy (mp) and source redundancy (ms) to improve the network efficiency .

The query arrival and data packet arrival event occurs each node performs clustering by using a clustering algorithm. The cost of redundancy management includes periodic clustering, intrusion detection and query processing through multipath routing .Finally we select the reliable path to route the data from source CH to a base station (sink) by using best redundancy level, path reliability, hop count.

```
Get next event
If event is  Timer then
Determine radio range to maintain  CH
    Determine ms, mp  and hop count
    Identify SNs  within the cluster for join process
else if event is query arrival then
     Perform multipath routing using ms, mp
else if event is   timer then
     Perform clustering
else if //event is finding unreliable node
    Sends feedback information to source CH
else // packet transmission
 Determine path reliability
Use geographic routing protocol design to forward the
packet and select optimized path for packet transmission
```

Fig. 2. CH execution for redundancy Management

```
Get next event
If event is  Timer then
Determine radio range to maintain   SN
Connectivity within a cluster
   Determine hop count
else if event is packet arrival from CH   then
    Update the settings using ms
else if event is   timer then
    Perform clustering
else if //event is finding unreliable node
    Sends feedback information to source CH
else // packet transmission
 Use geographic routing protocol design to
forward the packet and select optimized path for
packet transmission
```

Fig. 3. SN execution for redundancy Management

V. SIMULATION RESULTS

For simulation results we have used A X A area with 30 nodes .The nodes are distributed in the area using Poisson process .The initial energy levels of SN and CH nodes are ESN=0.8 joules and ECH=10 joules. The input parameter values are expressed in Table I.

Fig.4 shows packet reaching probability of three (mp ,ms) combinations such as (4, 3),(5,2) and (2,5).In above combinations (4,3) having highest reaching probability .By using Algorithm we can select the optimal redundant path by path reliability and hop count.

TABLE I

INPUT PARAMETER VALUES

Parameter	Value
n_b	50bits
N	25
r_{SN}	[5-25]m
r_{CH}	[25-100]m
$T_{clustering}$	60sec
T_D	[0.3-1]sec
f	1/4

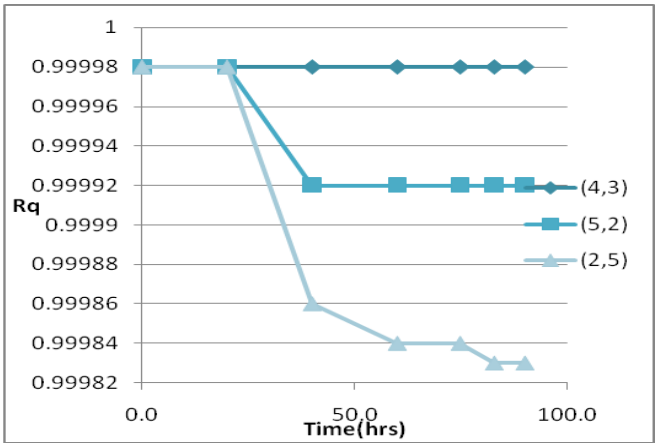

Fig.4 Reaching probability

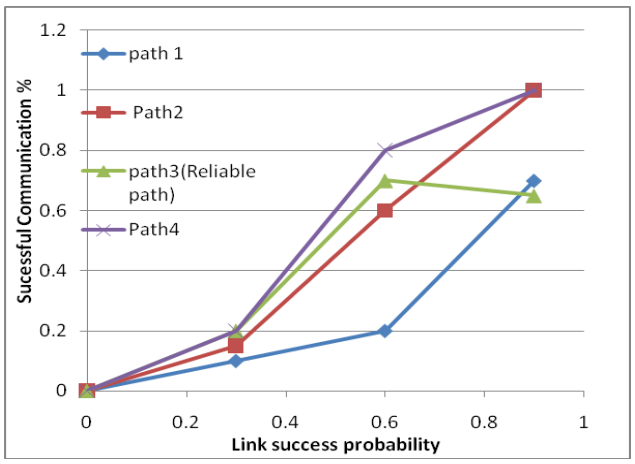

Fig 5. Link success probability with error rate

Fig.5 shows different links successful packet delivery. For 'choosing reliable path' problem our approach is compared with multiple paths in which reliable path having a low error rate and high packet delivery

VI. CONCLUSION

In this paper we performed trade off analysis between reliability vs. energy consumption for redundancy management of heterogeneous wireless sensor networks utilizing multipath routing to answer user queries .The proposed system is to find the redundancy level in terms of the path and source redundancy and intrusion tolerance settings in which the network lifetime is improved while satisfying reliability requirements .Finally we applied our analysis result in the design of redundancy management to identify and analysis the best design parameter settings at runtime to prolong the network efficiency .The reliable path is selected by using path reliability and hop count in the wireless sensor networks.

For future work, we plan to explore more extensive attacks and plan to investigate new protocols for selecting a reliable path to improve the network efficiency and also we will plan to do energy consumption techniques in heterogeneous wireless sensor networks.

REFERENCES

[1] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks:attacks and countermeasures," in *Proc. 2003 IEEE Int. Workshop SensorNetw. Protocols Appl.*, pp. 113–127

[2] T. He, J. Stankovic, C. Lu, and T. Abdelzaher, "SPEED: A Stateless Protocol for Real-Time Communication in Sensor Networks," Proc. IEEE Int'l Conf. Distributed Computing Systems, pp. 46-55,2003.

[3] E. Felemban, L. Chang-Gun, and E. Ekici, "MMSPEED: multipath multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 5, no.6, pp. 738–754, 2006.

[4] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Commun. Surveys & Tutorials*, vol. 10, no. 3, pp. 6–28,2008.

[5] E. Stavrou and A. Pitsillides, "A survey on secure Multipath routing protocols in WSNs," *Comput. Netw.*, vol. 54, no. 13, pp. 2215–2238,2010

[6] G. Bravos and A. G. Kanatas, "Energy consumption and trade-offs on wireless sensor networks," in *Proc. 2005 IEEE Int. Symp. Pers., Indoor Mobile Radio Commun.*, pp. 1279–1283.

[7] B. Hughes and V. Cahill, "Achieving Real-Time Guarantees in Mobile Ad Hoc Wireless Networks," Proc. Work-in-Progress Session 24th IEEE Real-Time Systems Symp., Dec. 2003.

[8] R. Chen, A. P. Speer, and M. Eltoweissy, "Adaptive fault-tolerant QoS control algorithms for maximizing network efficiency of query-based wireless sensor networks," *IEEE Trans. Dependable Secure Computing*,vol. 8, no. 2, pp. 161–176, 2011

[9] J. H. Cho, I. R. Chen, and P. G. Feng, "Effect of intrusion detection on reliability of mission-oriented mobile group systems in mobile ad hoc networks," *IEEE Trans. Reliab.*, vol. 59, no. 1, pp. 231–241, 2010

[10] H. Yousefi, A. Dabirmoghaddam, K. Mizanian, A.H. Jahangir, (2009) "Score Based Reliable Routing in Wireless Sensor Networks," IEEE 23rd International Conference on Information Networking.

[11] Hamid Al-Hamadi and Ing-Ray Chen,'*Redundancy Management of Multipath routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks*,' IEEE Trans. network and service management, *vol. 10, no. 2,2013*

[12] R. Machado, N. Ansari, G. Wang, and S. Tekinay, "Adaptive density control in heterogeneous wireless sensor networks with and without power management," *IET Commun.*, vol. 4, no. 7, pp. 758–767, 2010.