TOWARDS RELIABLE REACTIVE ROUTING IN INDUSTRIAL WIRELESS SENSORS NETWORKS

Supreeth Kumar M R
Visvesvaraya Technological University, Belgaum
Email: supreethmundur@gmail.com

Abstract- The control application of industrial wireless sensor networks (IWSNs) is subject to strict requirements in terms of reliable and efficient communication under fading channels. Transmission failures or deadline misses may seriously degrade the quality of control. In this project present the Reliable Reactive Routing Enhancement (R3E) to increase the resilience to link dynamics for IWSNs/WSNs. The R3E design method is to enhance existing reactive routing protocols to provide reliable energy-efficient packet delivery with less packet rejection ratio (PRR) against the unreliable wireless links by utilizing the local path diversity. Specifically, This implement a biased bakeoff timer scheme during the route-discovery phase to find a reliable guide path, which can provide more opportunities for cooperative forwarding. Along this path, data packets are greedily progressed toward the destination through nodes cooperation without utilizing the location information. Through extensive simulations results demonstrate that, while maintaining high energy efficiency and low delivery latency. R3E (R3E=1) remarkably show the less packet rejection ratio (PRR) compared to without R3E and encryption and decryption of the cooperative nodes.

Index Terms—Industrial wireless sensor networks (IWSNs),Encryption, Decryption, reliable forwarding, Unreliable wireless links.

I. INTRODUCTION

A). A Brief History of Wireless Sensor Networks

Wireless sensor networks (WSNs) is a wireless network consisting of spatially dispersed and dedicated autonomous devices that use sensors to monitor physical or external environmental conditions. A WSNs system is formed by combining these nodes or autonomous devices with gateway and routers.

The dispersed measurement nodes communicate wirelessly to a central gateway, the connection of a central gateway provides a connection to the wired world to where you can collect, analyze, process, and present your measurement data. The routers helps to gain an additional communication link between end nodes and the gateway for extend distance and reliability in a wireless sensor network. The networked structure of a wireless sensor is a scalable and requires very little power. It is also very smart, easy installation and easily programmable, and also capable of fast acquisition of a data, reliable in terms of transmission and accurate over the long term, but costs is less to purchase and install, and requires nearly zero maintenance. Simple block diagram of wireless sensor network communication shown in Fig.1.

Fig.1 A simple block diagram of wireless sensors networks.

B). Sensor Node

A Wireless Sensor Networks (WSNs) consists of spatially distributed sensor nodes and each sensor node can perform independently some processing and sensing tasks. In addition, sensor nodes communicate with each other in the form of order to forward their sensed information to a central processing unit or conduct some local coordination. The sensor node consists of several hardware components that include a radio transceiver, internal and external memories, an embedded processor, and one or more sensors, a geopositioning system, a power source. The architecture of sensor node as shown in Fig. 2.

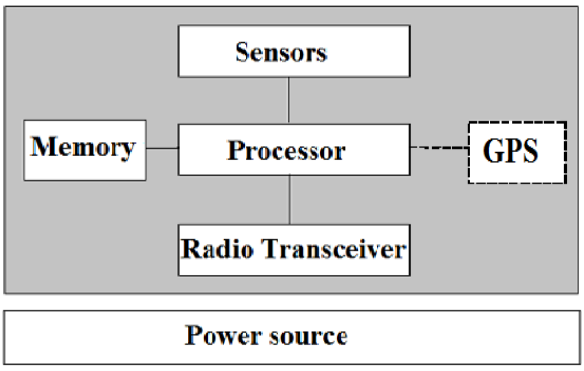

Fig.2 Architecture of sensor node.

The wireless sensor network devices primarily support only low-data-rate sensing, because limited bandwidth and power. There is various applications call for multi-nodal sensing, as a result each device may have several sensors on board. Depending upon the application requirements, several sensors are used such as temperature sensors, magnetometers, light sensors, humidity sensors, pressure sensors, chemical sensors, accelerometers, even low-resolution imagers, or acoustic sensors etc.

C). Related Work

Many reliability schemes have been investigated in literatures. The effect of on-demand behavior in routing protocols for multi hop wireless ad hoc networks was first proposed by *David A.Maltz, Josh Broch, jorjeta jetcheva, and David B, Johnson* [8]. The basic idea of their scheme was analyze the use of on-demand behavior in such protocols direction on its effect on the routing protocol's overhead cost, forwarding latency, and correctness of route caching, graph drawing examples from detailed simulation of the dynamic source routing (DSR) protocol.*Kan Yu, Mikael Gidlund, Johan Akerberg and Mats Bjorkman* [9] [10] proposed reliable real- time routing protocol for industrial wireless sensor and actuator networks. In this paper proposed for node weight values, control purpose and related node lists are utilized to provide directional information for wireless networks. Data packets forwarding is based on a controlled flooding mechanism with several forwarding criteria. [10] Proposed the reliable RSS-based routing protocol for industrial wireless sensor networks. In this paper, propose reliable and flexible received signal strength based routing scheme.*Filip Barac, Kan Yu, Mikael Gidlund, Johan Akerberg and Mats Bjorkman* [11] proposed towards reliable and lightweight communicatio-

-n in industrial wireless sensors networks. Address the issues of timeliness and transmission reliability of existing industrial communication standards, combine a forward error correction coding scheme on the medium access control layer with a lightweight routing protocol to form an IEEE 802.15.4-confortable solution.*Vehbi C. Gungor and Gerhard P.Hancke*[1] proposed industrial wireless sensor networks: challenges, design, and technical approaches. In this paper, first introduce the technical challenges and design principles are introduced in terms of hardware development, system architecture and protocols and software development. *Mahesh K.Marina and Samir R.Das*[4] proposed on-demand multipath distance vector routing in ad hoc networks. In this paper, develop an on-demand flooding scheme, multipath distance vector protocol for mobile ad hoc networks. Specifically, purpose multipath extensions to a

well studied single path routing protocol knows as ad hoc on-demand distance vector (AODV).

D). Proposed Work

This proposes a Reliable Reactive Routing Enhancement (R3E) to increase the resilience to link dynamics for WSNs/IWSNs. Our design inherits the advantages of opportunistic routing, thus achieving a less packet rejection ratio compared with existing routing, the cooperative node graph shows an encryption and decryption results to increase network security in wireless channel and reliability. R3E is designed to enhance existing reactive routing protocols to warfare the channel variation by utilizing the local path diversity in the link layer.

D). Motivation

Before providing the detailed design, first characterize the motivation behind R3E design. The idea of opportunistic routing is to utilize the path diversity for cooperative holding, that is, in each hop, neighboring nodes that hold the copies of a data packet serve as caches, thus the packet will be retrieve from any of downstream nodes. The rationale is that, the path with higher spatial diversity (more potential helper nodes) may possibly provide more reliable and less packet rejection ratio (PRR) against the unreliable links. With this observation, this aim is to find such a reliable virtual path to guide the packets to be progressed toward the destination. Call this virtual path a guide path, in which the nodes are named as guide nodes and increase the security by adopting an encryption and decryption to cooperative nodes. The general direction toward the destination points out from the guide path, and the node routing decision is made a posteriori, i.e., the actual forwarders are chosen based on the packet reception results at each hop.

II. MAIN DESIGN

A). Architecture Overview

The dependable receptive directing upgrade the reliable reactive routing enhancement (R3E) square structural planning shows in the Fig.3, which is a center product outline between the MAC and network layers to expand strength connection elements for WSNs/IWSNs.

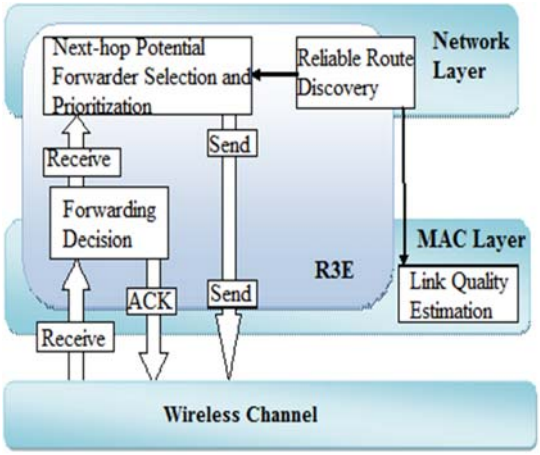

Fig.3 R3E architecture Overview.

The Fig.3, the R3E improvement layer comprises of three primary modules; there are reliable route discovery module, the potential forwarder determination and prioritization module, and the forwarding decision module. The potential forwarder and partner hub are entomb alterable. Before giving the outline, first this point is to locate the dependable guide way, as a result of more solid and effective parcel conveyance against the temperamental remote connections. Call this guide way a virtual way, in which the hubs are named as guide hubs. The Fig.4 illustration of the dependable guide way and actual way, in this guide hubs information to be advanced towards the destination. The Fig.4 [source→ 3→ 7 → Dest] is a guide way, and hubs 3 and 7 are the guide hubs. The guide way brings up the general bearing from source to destination, and the steering choice is made a back, i.e., the bundle gathering results at every jump, picked the real forwarders. When they are going to plan with and without R3E, the accompanying configuration strategies are vital.

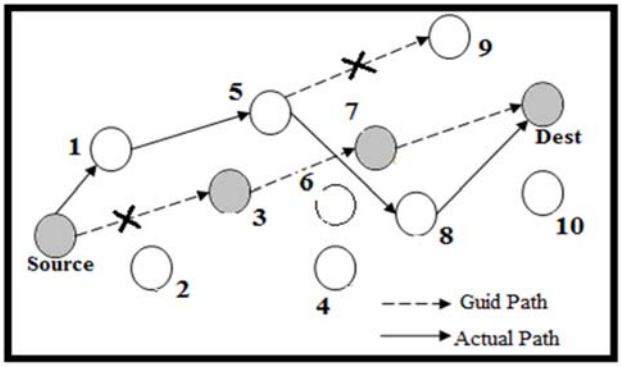

Fig.4 Example of the reliable guide way and actual path.

B). Reliable Route Discovery Module

The solid course reliable route discovery module, every hub included the system called agreeable sending procedure without using the area data and every hub do discovers and keeps up the course data for getting dependable directing. The course disclosure module has a two sorts a Route Request(RREQ) and Route Reply (RREP) system, both spread technique as a rule happens on prerequisites by spreading a RREQ(Route Request) through remote system, i.e., when a hub has an information parcels to send , it spread a RREQ. At the point when a data parcel route is found, the hub destination gives back a Route Reply, which includes the every bounce by-jump or course data or complete location from source to destination. The course disclosure module join the new expansion strategy for the helpful sending alongside the one-sided backoff clock plan, clarify in the following area.

C). Route Request (RREQ) Propagation

On the off chance that a hub has information parcels to send to destination from source, it will begin to starts a dependable course revelation by flooding a RREQ message. At the point when a hub gets a "non- copy RREQ", it stores the non-copy upstream hub id and course demand's succession number for converse route learning. The current responsive steering systems confront the same issues, it will be quickly rebroadcasting the RREQ. Another new technique, are going to receive the backoff clock plan at the current RREQ sending hub. The point of RREQ operation is to deliberately enhance the distinction of RREQ's navigating defers along distinctive
ways.

Accepting a RREQ message at the destination hub, i.e., in remote system there is no hub send a RREQ from source to destination, after destination answers a RREP message to source from destination. In a dependable steering, a destination hub is neglect to accepting a RREQ message from source, for this issue embrace a backoff clock plot in an agreeable sending method.Fig.5 demonstrate a case of a RREQ message headed out from source to destination and RREP message from destination to source. In Fig.5 demonstrates to took care of a hub with reliable (R3E = 1) and without reliable (R3E = 0), when R3E= 1, it will choose as per the need means minimum backoff clock for headed out RREQ from source to destination and RREP from destination to source.

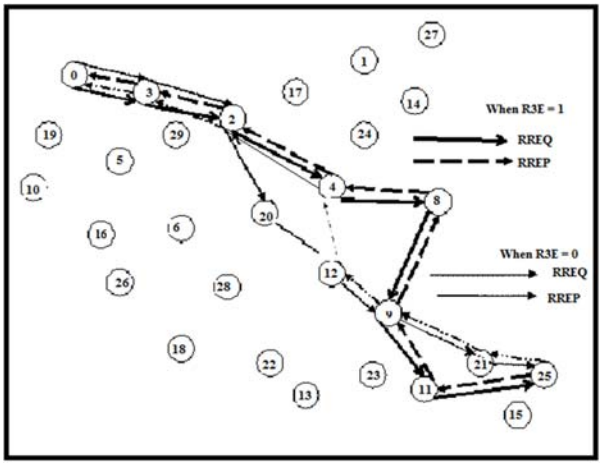

Fig.5 An example of a RREQ message travelled from source to destination and RREP message from destination to source of with and without reliable.

D). Route Reply (RREP) Propagation

At the point when a hub gets a RREP, it checks in the event that it is the chosen next-jump in the system (the upstream guide hub) of the RREP. In the event that is the situation, the hub acclimates that it is on the guide way from destination to the source and imprints itself as guide hub. At that point, the hub says its upstream guide hub ID for this RREP and advances it. In this way, the RREP is engendered by every guide hub until it achieves the source by means of the opposite course of the particular RREQ. At last, this system discovers guide way from the source to the destination.Fig.5 illustration demonstrates the RREP went from the destination hub to the source hub of both with and without reliable. In our outline, the RREP message has twofold capacities strategies. It not just consummate the forward way setup, i.e., stamping guide hubs along the opposite course, additionally illuminate the potential partners to elevate simple approach to agreeable sending. Especially, sets of two assistants and their transfer need assignments are incorporated in the RREP. Assume p_{i-1} , p_i, p_{i+1} and are three adjoining guide hubs, the upstream connection partner set $U(i-1,i)$ and downstream connection assistant set $U(i ,i+1)$, together with their packet reception ratio(PRRs) around the relating downstream guide hubs are piggybacked to the RREP when hub advances it. Because of the show way of remote correspondence, the majority of the guide hubs in $U(i-1, i)$ are figured

on to listen in this RREP. At the point when the aide hub p_{i-1} gets the RREP from p_i, it records its downstream guide hub pi, and *U(i-1, i)*. At the point when the upstream connection aides in *U(i-1,i)* get the RREP, they record p_{i+1} , *U(i ,i+1)* , p_i , and *U(i-1,i)*, which will be helpful in the information sending stage. Algorithm 2 portrays how a hub handles the RREP got from its downstream guide hub.

Since R3E is an upgrade layer over existing responsive directing conventions, the R3E banner bit is utilized to signify that the R3E capacity is engaged. There is no much convention for the RREQ message, where just the jump check is incorporated. R3E brings about a certain convention overhead in RREP, i.e., piggybacked an arrangement of hub IDs to the RREP, as indicated in Fig.6. Notwithstanding, the overhead will be in the end repaid by execution increase amid the information transmission stage. Assume the guide hub conveys a RREP to the upstream guide hub p_{i-1}, $(p_j \in U(i-1,i)$ and hub catches this message. This characterize the downstream hub set of p_j , signified by *SNS (j)*, as the successive hubs that rank in front of p_j in the piggybacked hub rundown of RREP. As seen in Fig.6, *M (j)* ∩ *SNS (j)* is the potential downstream guide set of p_j.

E). Forwarding Decision

The obligation of the sending choice module is a hub effectively gets information parcels, the sending choice module checks whether it is one of the deliberately beneficiaries. On the off chance that yes, this hub will store the approaching information parcel and begin backoff clock to give back an ACK (acknowledgement) message, where the information clock quality is connected with its positioning in the planned recipient rundown (called sending hopeful rundown). In the event that there is no such other rundown of forwarder hopeful with higher need transmitting an ACK before its backoff clock qualities lapses, it will transmit an ACK and convey the bundle to the upper layer, i.e., getting occasion in the system layer is trigger.

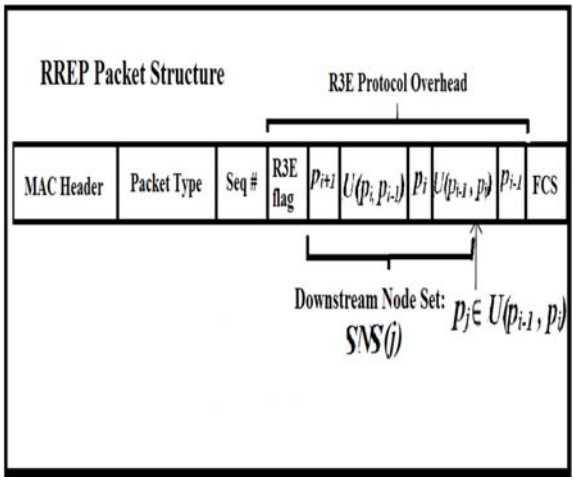

Fig.6 RREP packet structure.

F). Next–Hop Potential Forwarder Selection and Prioritization

The dependable of the potential forwarder determination and prioritization and sending choice module is runtime sending stage, in which it appends the requested forwarder rundown in the information parcels set out toward the following hub to hub. At long last, the current bundle will be submitted to the MAC layer and sent towards the destination.

F). Biased Backoff Scheme

Any hub that advances the Route Request (RREQ) will figure the backoff defer by accepting its self as a guide hub, and considering the last–hop hub as its upstream guide node.Fig.7 demonstrates a sample of a one-sided backoff timer.

Let Tij mean the backoff delay at the present sending hub p_i, which gets a RREQ from p_i. Tij is figured as characterized as.

$$\text{Tij} = \frac{Hop\ Count}{\sum_k X_{ik} X_{kj+1}} . \tau. \qquad p_k \in U(i,j) \tag{1}$$

Where τ is a period space unit; the *Hop Count* is the RREQ's bounce separation from the source hub hitherto. The basis is that, the neighbor with all the more sending applicants, better hub joins qualities for transmission of information, and additionally shorter bounce check will have a shorter backoff postponement to rebroadcast the RREQ.

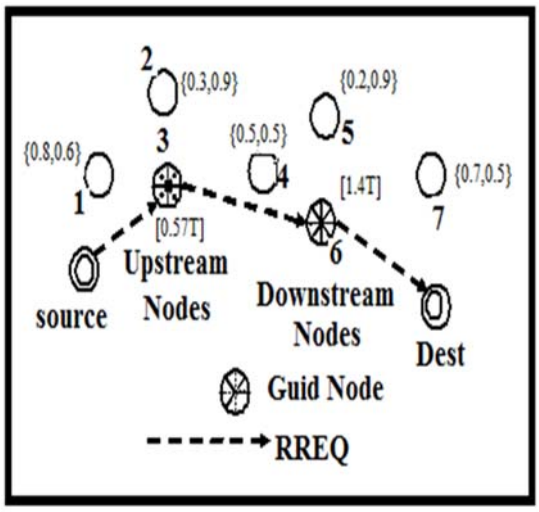

Fig.7 Example illustrating the biased backoff scheme for RREQ propagation.

Case in point, hubs 1, 2, and 3 get a RREQ from the source. At the point when hub 3 computes its backoff delay, it regarded itself as an guide hub and source as the upstream guide hub. From the nearby neighbor table, hub 3 realizes that 1 and 2 are partner hubs. At that point, it can do the ascertain the estimation of backoff postponement. In Fig. 3.5, the mark {0.8, 0.6} close to the assistant hub 1 implies that $X_{source1}$ = 0.8 and X_{13} = 0.6. At hub 3, the backoff deferral is about as indicated by (1). Contrasted and 1 and 2, 3 have a shorter backoff delay. At the point when 3's backoff clock first it lapses, the RREQ is retransmitted. Thus, hub 3 has a first higher need to forward the RREQ. Same system for next, hub 6 advances the RREQ before 4 and 5. Consequently, the RREQ course that goes along [Source→ 3 → 6] the way touches base at the *Dest* first. From (1), can see that the higher need is perhaps given to the way with more potential guides.

After accepting a RREQ message, a destination hub answers by sending a RREP message back to the source along the opposite course. In the event of getting the same RREQ message number of times, the destination hub should just answer to the initial.

G). Cooperative Forwarding

The helpful sending system in R3E is shown as takes after. The source hub telecasts a parcel, which incorporates the rundown of hub sending applicants (assistant hubs and the downstream guide hub) and their needs. Those sending hopefuls take after the allotted higher needs to hand-off the parcel. Every competitor, if having gotten the information bundle precisely, will begin a backoff clock whose worth relies on upon its need. The need of higher clock, the shorter is the clock esteem for information to transmit. The applicant whose clock lapses will answer with an ACK to advise the sender hub, and also to stifle other hub contenders in the system. At that point, it retransmits the information bundle toward its downstream connection. On the off chance that no such sending applicant has effectively gotten the information parcel, the sender will show the information bundle if the retransmission instrument is empowered.

From the reasonable connection conditions in remote systems, a potential forwarder with a higher parcel gathering proportion toward the downstream guide hub perhaps has a shorter separation from that guide hub, as more separations typically bring about lower got signal quality and in this manner expanded likelihood of bundle misfortune. Subsequently, the hand-off need standard is as per the following.

- At the point when an aide hub p_{i-1} transmits the information bundle, the downstream guide hub p_i has the most noteworthy need; and the partner hubs *U(i-1,i)* in are requested descendingly as per their PRRs toward p_i.
- Assume the downstream guide hub p_i neglects to get the information parcel, while a partner p_j in *U(i-1,i)* gets the bundle and takes the sending undertaking. The sending applicants of p_j are given by $M(j) \cap SNS(j)$.

All the more particularly, the sending competitor set of p_j is made out of three sections:

1) The partner hubs who have first higher needs than p_j in *U(i-1,i)*.
2) The downstream guide hub p_i.
3) $M(j) \cap (U(i,i+1) \cup \{p_{i+1}\}$.

To accomplish the base number of transmissions, the hand-off needs are requested as: Need of (3) > Priority of (2) > Priority of (1).

This demonstrates the assistant hubs and their needs at every bounce in the information sending stage in Fig.8(a). The partner hubs and their higher needs at the first jump are {3, 2, 1}. Assume guide hub 3 neglects to get the parcel accurately, while assistant 2 effectively gets the bundle, as demonstrated in Fig.8(b). B takes the sending undertaking rather than 3. At that point 2 upgrades its partner set as {4, 3} and advances the information parcel to its downstream

potential forwarders. It can be seen that R3E is strong to the remote connection motion.

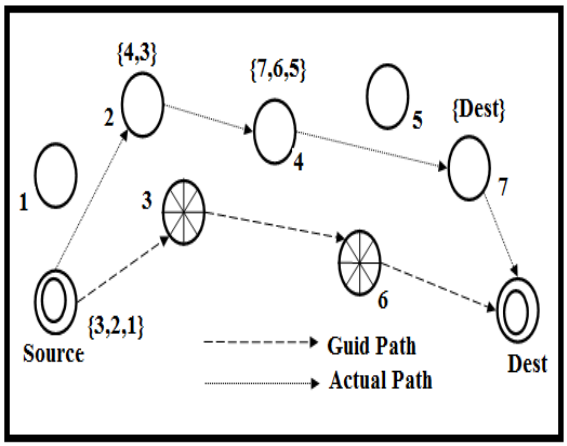

Fig.8 (a) Example illustrating the forwarding candidates and their priorities at each hop.

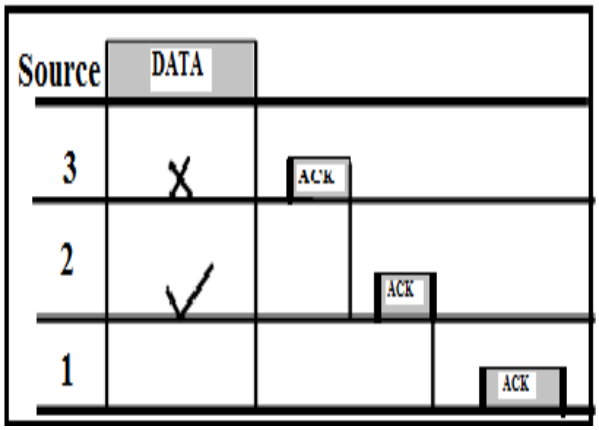

Fig.8 (b) Corresponding cooperative forwarding procedure at the first hop in the MAC layer.

H). MAC Layer

In this venture, the obligation of the MAC layer is the connection quality estimation. There has been a great deal of existing chip away at how to gauge remote connection quality in an exact and productive way. In this venture, two-beam ground model is received. The model gives more precise expectation at a long separation than the free space model. They got force is anticipated by:

$$P_r(d) = \frac{P_t G_t G_r h_t^2}{d^4 L} h_r^2 \quad (2)$$

Where P_t is the transmitted signal; G_t and G_r are the reception apparatus increases of the transmitter and the reception separately; L is the framework misfortune; d is the separation in the middle of transmitter and receiver; h_t and h_r are the statures of transmit and get receiving wires individually. In this paper, assume that the transmit scope of every hub is equal. Thus, the connection link quality $L_q = P_r$.

III ALGORITHM AND FLOWCHART

A). Algorithm

Let p_i and p_j mean the last-hub and present sending hub of a RREQ of source to destination, separately. Let *M(i)* symbolize the arrangement of p_i 's single bounce neighbors, and *DM(i,j)* speak to the normal kindred resident set in the middle of p_i and p_j. This characterize an guide hub p_k sandwiched in the middle of p_i and p_j as the across the board neighbor of p_i and p_j, pleasing $X_{ik} > X_{ij}$ and $X_{kj} > X_{ij}$, where X_{ij} is the PRRs in the middle of p_i and p_j . For cooperative routing, present exists an implied impediment, that is, the hubs in the colleague set must have the capacity to listen from one another with an influentially high likelihood. Let *U (i, j)* mean the arrangement of assistants including pi and p_j. As it were, *U(i, j)* is the general neighbor situated in the middle of p_i and p_j on the rule that any two hubs in *U(i, j)* can listen stealthily all other, and $\forall\ p_k \in U(i,j),\ X_{ik} > X_{ij},\ X_{kj} > X_{ij}\ U(i,j) \subseteq \{M(i) \cap M(j)\}$.

1). Route Request (RREQ) Propagation Algorithm

The Route Request (RREQ) propagation is explained in the earlier section.The algorithm 1 describes the outline of the Route Request process and how to handle the node, when receiving a request from source to destination. When a node accepting a non-duplicate request, it stores the upstream node id and RREQ's cycle number for reverse route learning. As a replacement for of rebroadcasting the RREQ in presented routing protocol in wireless networks. The algorithm 1 shows a node p_j, handles the RREQ accepting from node p_i..

2). Route Reply (RREP) Propagation Algorithm

The Route Reply (RREQ) propagation is explained in the earlier section. The algorithm 2 describes the outline of the Route Reply process and how to handle the node, when receiving a request from destination to source. Algorithm 2 shows a node p_j handles the RREP accepting from its downstream guide node p_i.

B). Flowchart

The working flowchart of both with and without R3E as shown in Fig.9. In this flowchart, a packet reception ratio (PRR) can be calculated as.

$$PRR=\frac{(Range-Distance)}{Range} \quad (3)$$

The flow chart of the without reliability (R3E=0) computation take place in the simulation. First of all write the source node and destination node, and mention the node range. The aim is to show the less packet rejection ratio (PRR) compared with unreliable protocol (without R3E) and encrypt and decrypt of the cooperative node to increase the resilience in industrial wireless sensor networks. This is the main working flowchart for the executing a network file (nam file).

IV PERFORMANCE EVALUATION

This section portrays the reenactments have finished to assess the execution of with reliability and without reliability convention. This think about the execution of both conventions. How the precision of connection dependability estimation will change the execution of R3E is additionally explored and demonstrates the agreeable hub of encryption
and decryption.

Algorithm 1: A node p_j handles the RREQ received from node p_i.

```
1   Procedure: void Recv RREQ (Packet *p)
2   if Non-duplicate RREQ then
3     if p_j is the destination node then
4       Send out RREP;// except introducer zone IDS=node;
5     else
6   DM(i,j) = M(i) ∩ M(j) ;
7   //get common neighbor set DM(i,j).p_k ∈ DM(i,j);
8    Sort DM(i,j) descendingly ordered by X_ik  X_kj  ;
9   U (i,j) = {dm1} , DM(i,j) = DM(i,j) – {dm1};
10   // dm1 is always the first item of DM(i,j);
11  While DM(i,j) ≠ Ø do
12   if Check Connectivity (U (i,j). cn1) then
13     // cn1 is within the transmission range of any
         node in U(i, j);
14     U(i,j) = U(i,j) ∪ { dm1};
15  end
16   DM (i ,j) = DM(i,j) -  dm1;
17  end
18  Calculate Bij and call Backoff (T_ij,p) ;
19 //schedule a timer whose value is T_ij , then call
   forward RREQ(p) when the timer expires;
20  end
21 else
22    Drop p;
23 end
```

Algorithm 2: A node p_j handles the RREP received from its downstream guide node p_i.

```
1   Procedure: void Recv RREP (Packet *p)
2   if Non-duplicate RREP then
3     if p_j = = p_i-1 then
4       // p_j is the selected next-hop & guide node p_i-1;
5       Mark myself as a guide node;
6       Record p_i and U (i-1, i);
7       Get RREP's next-hop node id p_i-1; //Except IDS=node
8       Attach, p_i, U(i-1,i),p_i-1  and U(i-2,i-1) to RREP;
9  /* p_i-2 is p_i-1's upstream guide node; the helper set
    is ordered descendingly by the PRR toward the
    downstream guide node;*/
10  Call forwardRREP p;
11    else if p_j ∈ U(i − 1, i)then
12     // p_j is a helper in U(i-1,i) ;
13     Record p_i+1, U(i ,i+1),p_i and U(i-1,i) ;
14  Drop p ;
15 else
16   Drop p;
17 end
18 else
19   Drop p;
20 end
```

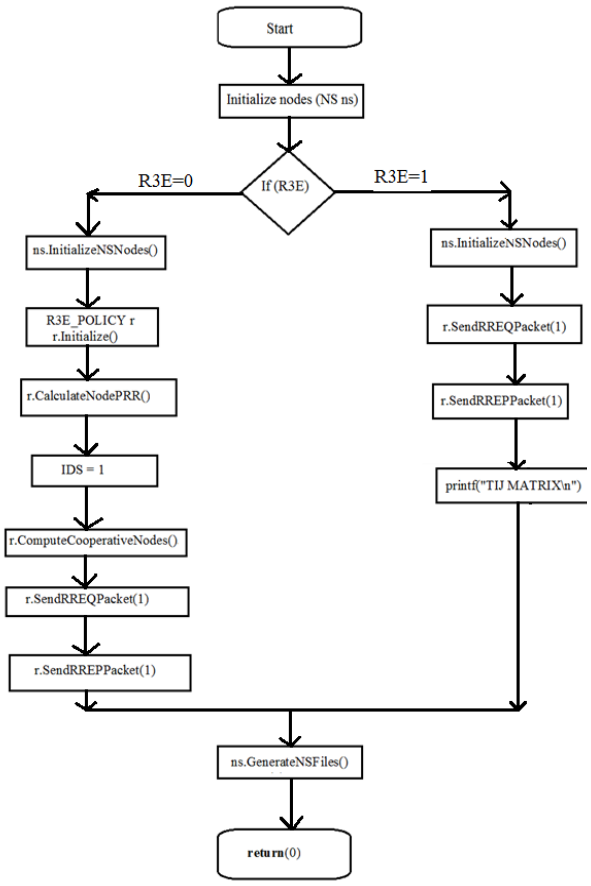

Fig.9 Flowchart of with and without reliable.

A). Simulation Setup

First the simulation set of connections for our experiments is described. In order to approximation the reliability performance, it is understood that no congestion and collision is involved and all the packet victims are caused by link failures due to node. This demonstrate the Packet Rejection Ratio (PRR) of both with and without R3E and cooperative node encryption and decryption results in three different scenarios. The packet rejection ratios defined as the number of packets that are dropped or lost due to congestion in the network. In the NS2, number of node is 30 and network diameter 6, HIGH_ QOS is 0.73 and LOW_QOs is 0.23, range is 100m and TX_Energy 2.0joules.

***Scenario 1*:** Fig.10(a) shows the NAM window of both with and without R3E. The black node 20 is the introducer zone to protect the packets. Node 0 (zero) is the source node and node 25 is the destination node, the blue color represents the represents the guide node and green node represents cooperative nodes and helper nodes. In the Fig. 10(a) black line indicates the without R3E RREQ from source to destination and dashed black line indicates RREP from destination to source. Another side yellow line indicates with R3E RREQ from source to destination and red line indicates the RREP from destination to source.

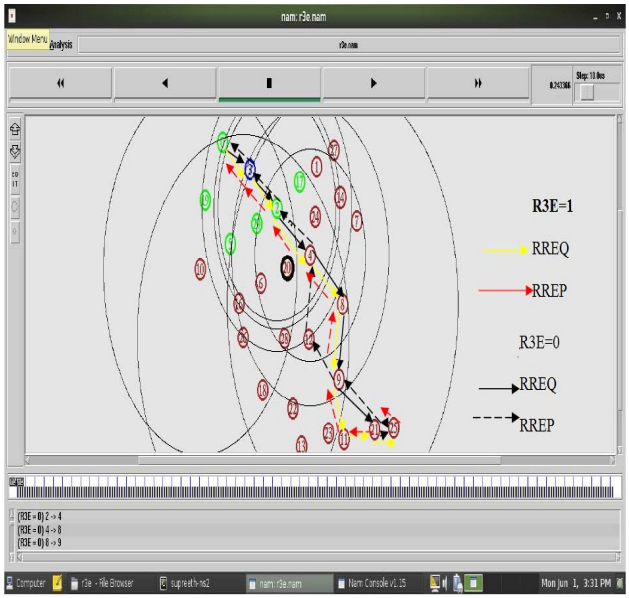

Fig. 10(a) NAM window (0-25).

Fig. 10(b) shows the Xgraph of both with and without R3E of the packet rejection ratio (PRR) v/s Iteration. In this graph with R3E achieve very less packet rejection compared with without R3E. Fig. 10(c) shows a cooperative node v/s node id for increase security purpose in with R3E and avoid malfunction of cooperative node.

Fig. 10(b) PRR v/s iteration of with and

without R3E (0-25).

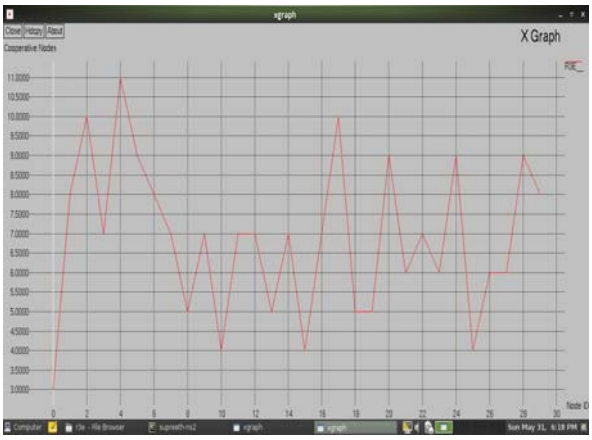

Fig. 10(c).Cooperative node v/s network id (0-25)

***Scenario 2*:** Fig.11 (a) shows the NAM window of both with and without R3E. The black node 4 is the introducer zone to protect the packets. Node 3 is the source node and node 15 is the destination node, the blue color represents the represents the guide node and green node represents cooperative nodes and helper nodes. In the Fig. 11(a) blackline indicates the without R3E RREQ from source to destination and dashed black line indicates RREP from destination to source. Another side yellow line indicates with R3E RREQ from source to destination and red line indicates the RREP from destination to source.

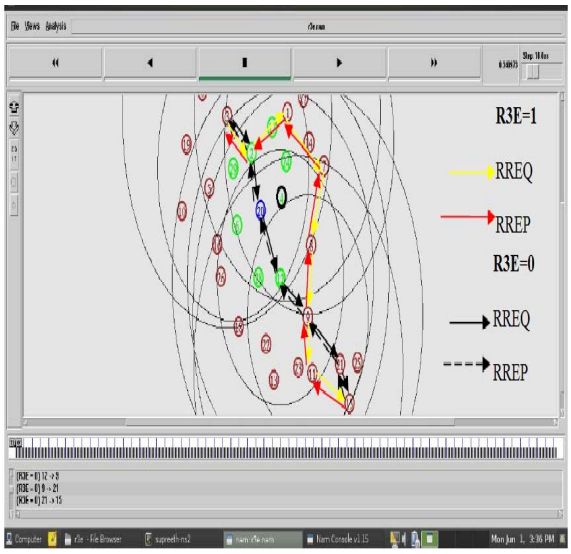

Fig. 11(a) NAM window (3-15).

Fig. 11(b) shows the xgraph of both with and without R3E of the packet rejection ratio (PRR) v/s Iteration. In this graph with R3E achieve very less packet rejection compared with without R3E. Fig. 11(c) shows a cooperative node v/s node id for increase security purpose in with R3E and avoid malfunction of cooperative node.

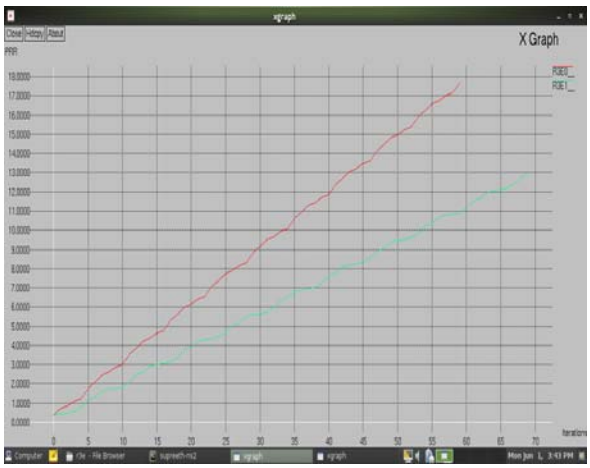

Fig. 11(b) PRR v/s iteration of with and without R3E (3-15).

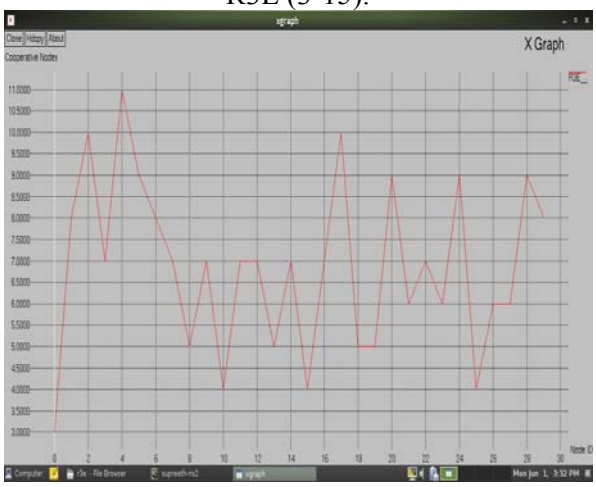

Fig. 11(c) Cooperative node v/s network id (3-15)

***Scenario 3*:** Fig.12(a) shows the NAM window of both with and without R3E. The black node 22 is the introducer zone to protect the packets. Node 0 (zero) is the source node and node 13 is the destination node, the blue color represents the represents the guide node and green node represents cooperative nodes and helper nodes. In the Fig. 12(a) black line indicates the without R3E RREQ from source to destination and dashed black line indicates RREP from destination to source. Another side yellow line indicates with R3E RREQ from source to destination and red line indicates the RREP from destination source.

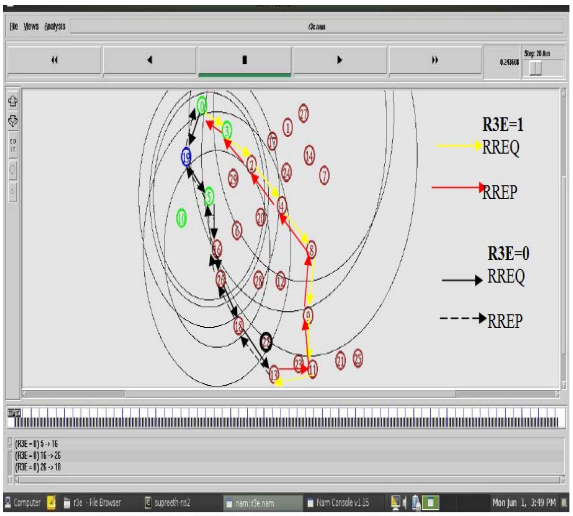

Fig. 12(a) NAM window (0-13).

Fig. 12(b) shows the xgraph of both with and without R3E of the packet rejection ratio (PRR) v/s Iteration. In this graph with R3E achieve very less packet rejection compared with without R3E. Fig. 12(c) shows a cooperative node v/s node id for increase security purpose in with R3E and avoid malfunction of cooperative node.

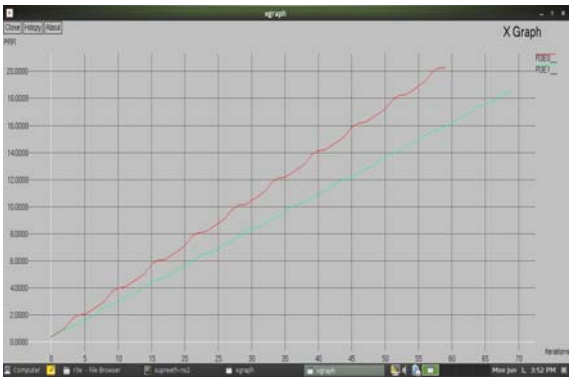

Fig. 12(b) PRR v/s iteration of with and without R3E (0-13).

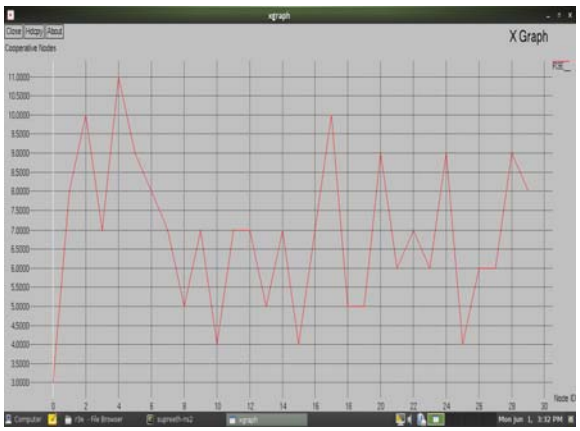

Fig. 12(c) Cooperative node v/s network id (0-13)

V. CONCLUSION

The R3E can enhance most presented reactive routing protocols in WSNs/IWSNs to present reliable and less PRR adjacent to the unreliable wireless links. A biased backoff clock has been introduced in the route discovery phase to find a healthy virtual path with less over-head. Without utilizing the location information, data packets can still be selfishly progressed toward the destination next to the virtual path. Therefore, R3E provides very close routing presentation, which demonstrate its effectiveness and feasibility. R3E (R3E=1) can effectively improve robustness and shows less packet rejection ratio along with cooperative node security v/s node id.

REFERENCES

[1]. V. Gungor and G. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[2]. S. eun Yoo, P. K. Chong, D. Kim, Y. Doh, M.-L. Pham, E. Choi, and J. Huh, "Guaranteeing real-time services for industrial wireless sensor networks with IEEE 802.15.4," *IEEE Trans. Ind. Electron.*, vol. 57, no. 11, pp. 3868–3876, Nov. 2010.

[3]. C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. IEEE WMCSA*, 1999, pp. 90–100.

[4]. M. Marina and S. Das, "On-demand multipath distance vector routing in ad hoc networks," in *Proc. IEEE ICNP*, Nov. 2001, pp. 14–23.

[5]. D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Computing*, pp. 153–181, 1996.

[6]. K. A. Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? the development of Ocari technology," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[7]. X. Huang, H. Zhai, and Y. Fang, "Robust cooperative routing protocol in mobile wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 5278–5285, Dec. 2008.

[8]. "U. D. of Energy, Industrial wireless technology for the 21st century," Office of Energy and Renewable Energy Report, 2002.

[9]. K. Yu, M. Gidlund, J. Åkerberg, and M. Björkman, "Reliable Real-time routing protocol for industrial wireless sensor and Actuator networks," in *Proc. IEEE*, 2013, pp. 1895–1901.

[10]. K. Yu, M. Gidlund, J. Åkerberg, and M. Björkman, "Reliable RSS-based routing protocol for industrial wireless sensor networks," in *Proc. IECON*, 2012, pp. 3231–3237.

[11]. F. Barac, K. Yu,M. Gidlund, J. Akerberg, andM. Bjorkman, "Towards reliable and lightweight communication in industrial wireless sensor networks," in *Proc. IEEE INDIN* , 2012, pp. 1218–122.