ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Survey on Industrial Wireless Sensor Networks

Pavithra L, Angeline A

M.Tech, Dept of ISE, The Oxford College of Engineering, Bangalore, India.

Asst. Prof, Dept of ISE, The Oxford College of Engineering, Bangalore, India.

ABSTRACT: Wireless sensor network have benefits, due to their large benefits in terms of faster installation, lower cost, and flexible. Wireless sensor network operate in license-free Industrial Scientific and Medical(ISM) band hence share the spectrum with other technologies. In IWSN link failure occur because of multipath propogation from metallic surfaces, excessive electromagnetic noise and asymmetric capabilities. However, for industrial applications, new requirements such as reliable (in-time) delivery is a main constraint. A survey on industrial wireless sensor networks is presented.

KEYWORDS*:* Industrial wireless sensor networks; opportunistic routing; unreliable wireless links; cross-layer design.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are adopted in the industrial world due to their advantages over wired networks. Industrial Wireless Sensor Networks (IWSNs) offer several advantages like easy and fast installation and lowcost maintenance [1]. IWSN applications, such as factory automation, industrial process monitoring and control, and plant monitoring, which require reliability and timeliness in forwarding messages among nodes [2].Industrial wireless channel condition is considered to be harsh and dynamic due to metallic surfaces, extreme temperature, high vibrations and non-line-of-sight (NLOS) communications, interference issues, and other constraints [6]. When IWSNs are deployed in a hash industrial environment, the vulnerability of wireless signal leads to high risk of transmission failure and then results in missing or delaying of process or control data. in terms of money, man power, time and even human lives. However, for industrial automation, missing the process or control deadline is intolerable, which may terminate industrial application and finally result in disasters in terms of money, human lives, and time. Therefore, traditional routing protocols, such as AODV [3], AOMDV [4] and DSR [5], may find their limitations in industrial installations.

Since wireless medium is being shared, each node can overhear the data packet sent by its neighbors. The idea of opportunistic routing [10] is used to take the advantage of the broadcast nature of wireless communication, involving multiple neighbors of the sender into local forwarding and these neighbor nodes can find a reliable and energy-efficient path in case of link breakage. Since these neighbor nodes keep the copy of the same packet with no additional cost. In the case of actual path breakage these neighbor nodes can cooperatively forward the packet to its downstream neighbors.

II. RELATED WORK

There are different routing mechanisms, in WSN which include flooding-based, dynamic routing table-

based, clusterbased, geographical and self-organizing schemes. Among them, cluster-based and self-organizing routing schemes are mostly used for adhoc network, so they are not appropriate solutions for centralized IWSNs. Geographical routing protocols are usually designed for energy constrained purpose without considering reliability and latency. Therefore, flooding-based and dynamic routing table-based schemes are considered as potentially available solutions for IWSNs.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

A. Ad-hoc On De-mand Distance Vector Routing (AODV)

Perkins and E. Royer [4] proposed Ad-hoc On De-mand Distance Vector Routing (AODV). It is based on the combination of DSDV and DSR. In AODV, when source node S wants to send a data to a destination node D and does not have a route to D, it starts route discovery by broadcasting a route request (RREQ) to its neighbors. The neighbors who receive this RREQ rebroadcast the same RREQ to their immediate neighbors. This process is repeated unless and until the RREQ reaches the destination node D. On receiving the first inwards RREQ, the destination node sends a route reply (RREP) to the source node through the reverse path from where the RREQ arrived. If the same RREQ arrives later, it will be overlooked by the destination node. In addition, AODV enables intermediate nodes that have sufficiently fresh routes (with destination sequence number equal or greater than the one in the RREQ) to generate and send an RREP to the source node.

B. EARQ (energy aware routing for real-time and reliable communication in wireless industrial sensor networks)

J. Heo, J. Hong and Y.Cho proposed in [8] EARQ (energy aware routing for real-time and reliable communication in wireless industrial sensor networks). It is a proactive routing protocol that aims to maintain an ongoing routing table. In EARQ, each node calculates the energy, delay and reliability of a path toward the sink node. It selects a path that consumes less energy and the paths that deliver a packet in time. The maximum tolerable packet delay, is calculated based on the density of the sensor nodes and the radio range. EARQ sends a redundant packet through an alternate path if reliability of a path is less than a predefined value. EARQ also requires global accurate positioning information to perform the routing tasks and to calculate some of the route selection metrics. It does not consider the properties of WSNs such as the buffer size limitation of the sensor nodes.

C. Robust Cooperative Routing Protocol (RRP)

Huang, H. Zhai and Y.Fang proposed in [9] RRP (Robust Cooperative Routing Protocol) is a cross-layer robust routing protocol based on node cooperation among neighboring nodes for unreliable wireless sensor networks. Nodes work cooperatively to increase the robustness of routing against path breakage. It improves performance significantly in presence of node mobility and link error. Neighboring nodes can overhear the packet due to the broadcast nature of the wireless medium. This is shown in Fig. 1. As the neighbor nodes can overhear the next-hop node could retrieve the packet from any of the neighbors.

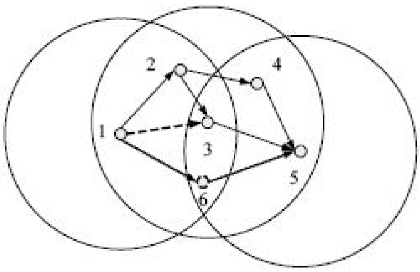

Fig.1. Actual path with equivalent or virtual nodes.

Inside the robust path expanded from an actual path, a reliable path is selected for packet delivery.

D. Dynamic Source Routing (DSR)

D. B. Johnson and D. A. Maltz [6] proposed Dynamic Source Routing is a source based reactive routing protocol. It is based on link state algorithm. It maintains a route cache. It uses route discovery and route maintenance processes. In this protocol, when the source node wants to communicate with another node then it checks the route cache for the availability of route to that node. If the route is not found in route cache or if it contains the expired route then route discovery process is initiated by sending route request packets (RREQ). Route maintenance process uses error messages and acknowledgement for maintenance of routes. If any link to source node is broken then an error message (RERR) is sent to the source node. DSR does not use HELLO packets. There is no need of keeping routing tables. It

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

supports multiple paths to a destination but it is not scalable to large networks.

E. Lightweight Routing Protocol

Barac, K.Yu,M idlund, J. Akerberg and Bjorkman presented in [10] a lightweight routing protocol for industrial wireless sensor network. It is a distributed approach, each intermediate node decides whether to retransmit or discard the packet received. Information for making the forwarding decision is derived from the data packet, so there are no control messages exchanged between the nodes. Each and every node should store the identifiers of the seen packets in order to identify the duplicate packets. The fields like packet age, TTL (time-to-live) are checked at every hop and outdated packets are removed. The weight of the node is used in order to progress the packet towards the sink. This protocol is capable of delivering data efficiently with low latency and has less complexity; latency is dependent on size of the network and the sensor refresh rate. It does not consider the buffer size of the sensors and it is not energy efficient.

II. APPROACH 1

The Fig. 2 illustrates the flowchart of the proposed system, which is a middle-ware design across the MAC and the network layers to cope up with the changes in link dynamics for WSNs/IWSNs. It consists of three main modules

1. Reliable Route Discovery Module,
2. Forwarding Decision Module.
3. Potential Forwarder Selection and Prioritization Module

Reliable Route Discovery Module

The reliable route discovery module finds the route between source and destination. During the route discovery phase, each node involved in the forwarding process stores the downstream neighborhood information, that is to say, when a node serves as a forwarder, it already knows the next-hop forwarding candidates along the discovered path based on the PRR(delay Parameter) the next hop is selected.

Forwarding Decision Module

This module is responsible at the runtime forwarding phase. After the route is established when the source starts sending the data packet, this module will check whether it is a actual receiver. If yes the node will store the packet and starts a timer to return the ACK. If there is no other forwarder candidate with higher priority transmitting an ACK before its timer expires, it will broadcast an ACK and deliver the packet to the upper layer, i.e., trigger a receiving event in the network layer.

Potential Forwarder Selection and Prioritization Module

This module is responsible at the runtime forwarding phase and attaches the ordered forwarder list in the data packet header for the next hop. Finally, the outgoing packet will be submitted to the MAC layer and forwarded towards the destination.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

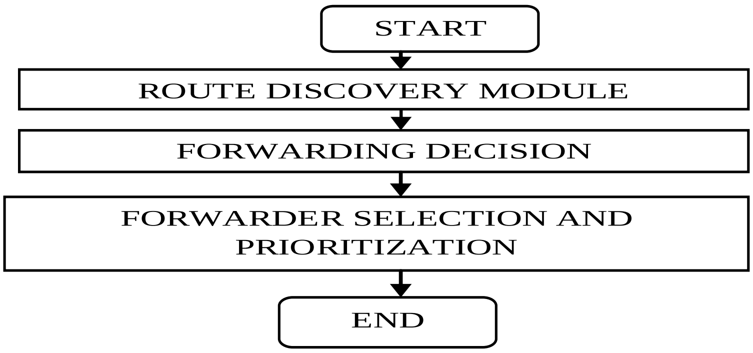

Fig.2. Flowchart of the proposed system

Let tij the backoff delay at the current forwarding node, which receives an RREQ from vi. vi and vj is the last hop and the current RREQ forwarding node then tij is calculated as defined in “(1)”,

$$t_{ij} = \frac{\text{HopCount}}{\sum_k P_{ik}P_{kj} + 1}, \ \tau, \ v_k \in H(i, j) \quad (1)$$

where τ is a time slot unit; the HopCount is the RREQ’s hop distance from the source node thus far. H(i,j) is the hepler set between vi and vj..Pik is the PRR(Packet reception ratio)between i and k , Pkj is the PRR(Packet reception ratio)between j and k The rationale is that, the neighbor with more forwarding candidates, better link qualities, as well as shorter hop-count will have a shorter backoff delay to rebroadcast the RREQ. Fig. 3 illustrates the biased backoff scheme.

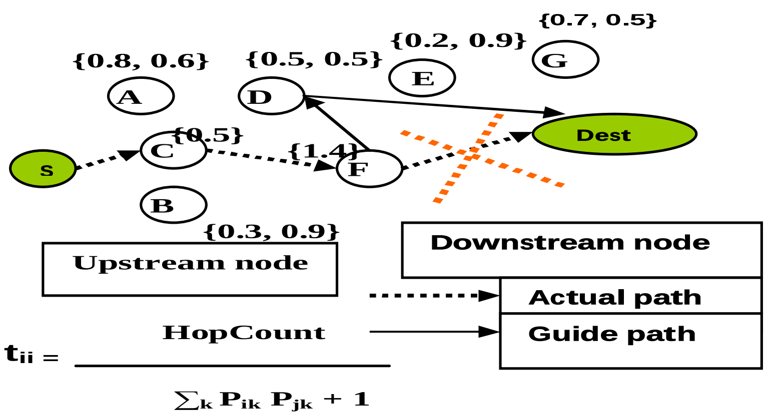

Fig.3. Example of the biased back-off scheme during the route discovery.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Any node that forwards the RREQ will calculate the backoff delay by assuming itself as a guide node, and considering the last-hop node as its upstream guide node [1]. After data transmission the sender waits for the ACK. If the actual receiver receives the data packet correctly then it will send an reply message after Short Inter Frame Spacing SIFS) or else the channel is idle in this period. The guard node (neighbor node) will learn that the actual link is being failed so it will send the ACK to the sender and transfer the packet to the downstream node.

III. APPROACH 2

In this approach we apply biased backoff scheme with DSR routing protocol. Here the source route is divided into three equal regions i.e. the source and destination regions which are of equal size and the middle region will be larger than the other two regions as shown in the fig. 4. If link failure occurs and if it is near the source node then route error message will be sent, if the failure is near the destination or in the

middle region then the relay node will search in its cache for other route to destination which has a shorter delay and also maximum energy level of the node and selects that node to route the packet to the destination and inform the source about the route change.

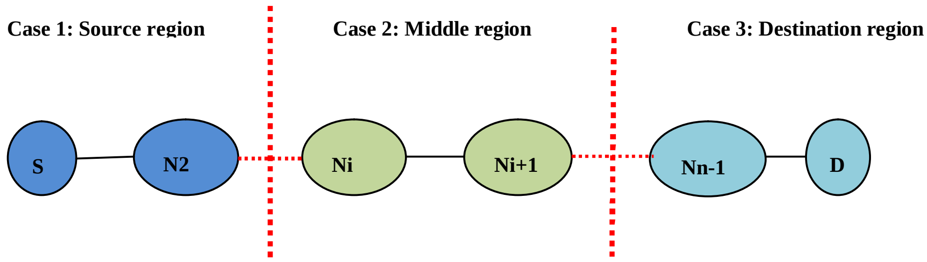

Fig. 4. Partition of the source route

IV. COMPARATIVE ANALYSIS

Biased backoff scheme applied during the link failure to both AODV and DSR. The performance of this is better than normal AODV and DSR. When considering the security issues and VANETS, DSR is better than AODV.

V. CONCLUSION

Biased back-off scheme is used along with the DSR routing protocol to provide a reliable path in the unreliable wireless link. So this scheme may provide more reliable and energy-efficient path because of no retransmissions then AODV.

REFERENCES

1. Jianwei Niu, Long Cheng, Yu Gu, Lei Shu and Sajal K. Das “R3E:Reliable Reactive Routing Enhancement Routing Protocol for Wireless Sensor Network “, IEEE Trans. Ind. Informatics, vol.10, no. 1,Feb. 2014.
2. 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.
3. 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.
4. C. Perkins and E. Royer, “Ad-hoc on-demand distance vector routing,” in Proc. IEEE WMCSA, 1999, pp. 90–100.
5. M. Marina and S. Das, “On-demand multipath distance vector routing in ad hoc networks,” in Proc. IEEE ICNP, Nov. 2001, pp. 14–23.
6. D. B. Johnson and D. A. Maltz, “DSR: Dynamic source routing in ad hoc wireless networks,” Mobile Computing, pp. 153–181, 1996.
7. 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

8. J. Heo, J. Hong, and Y. Cho, "EARQ: Energy routing for real-time and reliable communication in wireless industrial sensor networks" IEEE Trans. Ind. Inf., vol. 5, no. 1, pp. 3–11, Feb. 2009.
9. 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.
10. F. Barac, K. Yu,M. idlund, J. Akerberg, andM. Bjorkman, "Towards reliable and lightweight communication in industrial wireless sensor networks," in Proc. IEEE INDIN , 2012, pp. 1218–1224.
11. S. Biswas and R. Morris, "ExOr: opportunistic multi-hop routing for wireless networks," in Proc. ACM SIGCOMM, 2005, pp. 133–144.
12. J. Akerberg, M. Gidlund, and M. Bjorkman, "Future research challenges in wireless sensor and actuator networks targeting industrial automation," in Proc. IEEE INDIN , 2011, pp. 410–415.