www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 5 Issue 09 September 2016 Page No.17889-17893

Secure Reliable Reactive Routing Enhancement In Wireless Sensor Networks

Akash Joshi[1], Dr. Shiva Murthy G[2]

[1] VTU-Centre for PG Studies, Bengaluru Region, Bengaluru, India

joshiakash880@gmail.com

[2] VTU-Centre for PG Studies, Bengaluru Region, Bengaluru, India

kgshivam@gmail.com

Abstract: ***Rendering reliable and efficient communication along with security under losing channels is one among the major technical challenges in wireless network, especially in industries with vital and severe environments. In this task, illustrated a scheme to raise the resilience to link dynamics for Wireless Web, R3E is designed to enhance existing reactive course-plotting protocols to provide reliable and energy-efficient packet delivery against the unreliable cordless links by utilizing the local path diversity. Security is the major challenge with the R3E approach. Security with R3E is to be rendered with the range of the threshold, calculated at every node in the network. Proposed mechanism confirms reliable and secure path from source to destination by removing malicious nodes in the network.***

Keywords: WSNs, Reliable Routing, secure Routing, Secure Reactive Routing

1. Introduction

Wireless Sensor Network (WSN) are replacing the wired communication systems in the industries cause of several advantages such as timeliness, monitoring, control and automation, low maintenance cost, easy and fast installations [1]. Traditional routing protocols have their limitations in industries because of interference issues, harsh environment and many others constraint [2], [3].

In WSN routing may be a terribly difficult drawback owing to the inherent characteristics that differentiate such networks from alternative wireless networks. In recent years, several algorithms are planned for the routing protocols such as AODV [4], DSR [5] in wireless detector networks. In existing bestowed the sweetening R3E to extend the resilience to link dynamics for WSNs/IWSNs. R3E is meant to reinforce existing reactive routing protocols [14], [15], [16] to supply reliable and energy efficient packet delivery against the unreliable wireless links by utilizing the native path diversity [6]. To maximize the network survivability by mistreatment equal energy among as several nodes as potential. R3E remarkably improves the packet delivery ratio, while maintaining high energy efficiency and low delivery latency [17].

Routes are generally created and maintained by two different phases, namely: route discovery and route maintenance. Route discovery usually occur on-demand by flooding a RouteRequest(RREQ) through the network, i.e., when a node has data to send, it broadcasts an RREQ. When a route is found, the destination returns a RouteReply(RREP), which contains the route information traversed by the RREQ [7].

RouteRequest (RREQ) Propagation, if a node has data packets to send to a destination, it initiates a route discovery by flooding an RREQ message. When a node receives a non-duplicate RREQ, it stores the upstream node id and RREQ's sequence number for reverse route learning. Instead of rebroadcasting the RREQ immediately in existing reactive routing protocols, introduced a biased backoff scheme at the current RREQ forwarding node. Biased backoff scheme is to find an alternative route, when every the already established route fails.

RouteReply (RREP) Propagation, when a node receives an RREP, it checks if it is the selected next-hop (the upstream guide node) of the RREP. If that is the case, the node realizes that it is on the guide path to the source, thus it marks itself as a guide node. Then, the node records its upstream guide node ID for this RREP and forwards it.

The reliable route discovery module finds and maintains the route information for each node. During the route discovery phase, each node involved in the cooperative 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. The other two modules are responsible for the runtime forwarding phase. When a node successfully receives a data packet, the forwarding decision module checks whether it is one of the intended receivers. If yes, this node will cache the incoming packet and start a back-off timer to return an ACK message, where the timer value is related with its ranking in the intended receiver list (called forwarding candidate list). If there is no other forwarder candidate with higher priority transmitting an ACK before its back-off 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.

With this observation, aimed 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. Although there is a large research effort in the area of WSNs, many research issues have not been well addressed such that WSNs can be adopted properly for industrial automation. Akerberg [8], discuss major requirements for typical WSN applications in process automation and outline the research direction for IWSNs.

The remainder of this work is organized as follows. Section II describes the related works. Section III presents secure reliable reactive routing. Section IV provides the results and discussion. Finally, Section- V concludes the paper along with future work.

2. Related Works

Providing security and reliability to the data routing in WSNs is a challenge. There are lots of efforts being done to provide reliability to WSNs routing protocols. This section discusses on work carried out in recent past on security and reliable data routing.

K. Yu, M. Gidlund [9] et al, focuses on the IWSN rather than the use of automation in the industry. Because of the less features given by the industrial automation, and its less flexibility pushes us to use the IWSN in the industries. IWSN can give the better results rather than that of automation but the problem is that they can undergo transmission failures.

In the industrial automation, IWSNs have been increasingly applied due to a great number of benefits such as convenient installation, flexible deployment and cost efficiency. Compared with conventional wireless systems, IWSNs have more stringent requirements on communication reliability and real time performance. However, IWSNs are frequently deployed in harsh industrial environments with electromagnetic disturbances, moving objects and non-line-of-sight (NLOS) communication. Because of the vulnerability of the wireless signal, IWSNs are under high risk of transmission failures, which may result in missing or delaying of process or control data. For industrial automation, missing the process or control deadline is intolerable, which may terminate industrial application and finally result in economic loss and safety problems.

From hierarchy point of view, the high reliability and low latency can be achieved from different network layers. On MAC layer, existing protocols in IWSNs provide automatic repeat request (ARQ) to improve reliability at the cost of real time performance. An alternative method is to use Forward Error Correction (FEC) mechanism to provide more reliable transmissions and reduce the number of acknowledgement messages by recovering erroneous data.

F. Barac [10] et al, focus is about the networks with sensors and actuators, with some time constraint. This kind of system puts the concern to the reliability of the delivery of data. It also depicts the data flooding in the network. And also evaluates the potentials of flooding as a data dissemination technique in network.

The applications of Industrial Wireless Sensor and Actuator Networks (IWSAN) are time-critical and subject to strict requirements in terms of end-to-end delay and reliability of data delivery. A notable shortcoming of the existing wireless industrial communication standards is the existence of overcomplicated routing protocols, whose adequacy for the intended applications is questionable. This paper evaluates the potentials of flooding as a data dissemination technique in IWSANs. The concept of flooding is recycled by introducing minimal modifications to its generic form and compared with a number of existing WSN protocols, in a variety of scenarios. The simulation results of all scenarios observed show that our lightweight approach is able to meet stringent performance requirements for networks of considerable sizes. Furthermore, it is shown that this solution significantly outperforms a number of conventional WSN routing protocols in all categories of interest.

J. Akerberg [11] et al, focus on incorporating WSN in any industry. The advantage is in using WSN, how to use it in the industrial automation. Some major requirements are to be accomplished, by all the application in their automation. And some issues need to be taken care off.

A growing trend in the automation industry is to use wireless technologies to reduce cable cost, deployment time, unlocking of stranded information in previously deployed devices, and enabling wireless control applications. Despite a huge research effort in the area of WSNs, there are several issues that have not been addressed properly such that WSNs can be adopted properly in the process automation domain. This article presents the major requirements for typical applications in process automation and also aim to outline the research direction for IWSNs in industrial automation. The major issues that need to be addressed are safety, security and availability before industrial wireless sensor networks will be adopted in full scale in process automation.

K. Zeng [12] et al, focus on designing an energy-efficient and energy-aware real-time routing algorithm aiming to explore the long lifetime routing schemes in which delay constraint is satisfied in the presence of loss-y communication links. To achieve this goal, our energy-aware forwarding protocol utilizes an optimum distance real-time routing algorithm to minimize energy consumption in unreliable WSNs.

Lifetime is the most important concern in WSNs due to limited battery power of sensor nodes. Moreover, a WSN should be capable of timely fulfilling its mission without losing important information in event-critical applications. Simulation results reveal that the proposed algorithm outperforms other existing schemes in terms of energy consumption, network lifetime, and miss ratio. The tendency to use high performance low cost products in wireless communications technology has led to the rapid development of wireless sensor networks. Considering that communication costs (transmission power) are usually more than computing costs, energy efficient routing algorithms are very important in multi-hop WSNs where the constituent nodes have batteries with limited energy.

To achieve these objectives, each neighboring node is assigned a probability of being selected to forward a packet provided it satisfies the real-time requirement. This probability is a function of three parameters: the residual node energy, the distance to the straight path between the current node and the sink, and the effective transmission energy cost which includes the energy spent in potential retransmissions.

Sajal K. Das [13] et al, focus on re-routing which is reactive along with providing the reliability in the WSN. Reactive

routing is formerly based on the co-operative forwarder node, this node acts as medium while transmission.

R3E works to increase the resilience to link dynamics for WSNs/IWSNs. Our design inherits the advantages of opportunistic routing, thus achieving shorter end-to-end delivery delay, higher energy efficiency, and reliability. R3E is designed to augment existing reactive routing protocols to combat the channel variation by utilizing the local path diversity in the link layer. An overview of the functional architecture of R3E, which is a middle-ware design across the MAC and the network layers to increase the resilience to link dynamics for WSNs/IWSNs. The R3E enhancement layer consists of three main modules, the reliable route discovery module, the potential forwarder selection and prioritization module, and the forwarding decision module. The helper node and potential forwarder are interchangeable.

R3E majorly focuses on how to re-route in a case of link or node failures in the WSN's. What if there is a malicious node in the network which tries to modify the data, without forwarding it to the next node. This is a Denial of Service with selective forwarding which can lead to destination to get irrelevant data or no data in the worst case. So there is a need for providing security with R3E approach.

Security with R3E is provided with the help of threshold values. Minimum and maximum threshold values are initialized formerly. At every node threshold is calculated, and should fall within the range between minimum and maximum. Any node failing to do so, it is identified as the malicious node. Once malicious node is found out then is removed. Likewise security is to be provided with the R3E.

3. Secure Reliable Reactive Routing

R3E layers consists of the three parts which are, reliable route discovery part, potential forwarder selection and prioritization part along with decision for forwarding part. Potential forwarder is a helper node. The reliable route discovery part finds and also maintains the routing information of each node. It also information of adjacent nodes participating in co-operative forwarding, it also knew the node acting as the forwarder. It also knew the next node participating the actual path. The other nodes are responsible for runtime forwarding part. When any node receives the message, it first checks whether it is the intended receiver, if yes it sends the acknowledgement for that received message. If there is no other forwarder candidate with higher priority transmitting an ACK before its back-off 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. Then, the potential forwarder selection and prioritization module 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.

3.1 Security with R3E

Security with R3E adopts selective forwarding mechanism, which is one kind of a routing attack in sensor networks. Routing in R3E must by-pass this attack in the network. It is done in accordingly; malicious node is identified first, later on removed from that network.

Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion and unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

Malicious node makes DoS or sometimes even worse, so those kinds of nodes must be removed from the network. Selective Data Forwarding a kind of denial of service. A malicious node can selectively drop only certain packets. Especially effective if combined with an attack that gathers much traffic via the node

Once the guide paths are identified in the network, any node that is dropping the packets of data in a large number is identified as the malicious node. Below algorithm describes to detect the malicious node, PDR_{min} defines the minimum threshold and PDR_{max} defines the maximum threshold for identifying malicious node. PDR^{i}_{cur} defines the threshold value for the current node, which is calculated as shown in the below algorithm and $n \in N$ is the nodes present in the network. Initial assumption for PDR_{min} is 0.7 and PDR_{max} is 1.0 is made.

Algorithm to detect malicious node is:

1. Initialize PDR_{min}, PDR_{max}
2. For all $i \in \{n_1, n_2, \ldots n_m\}$
3. Calculate PDR^{i}_{cur} = (Packet_Sent / Packet_Recieved)
4. If (($PDR_{min} < PDR^{i}_{cur}$) && ($PDR^{i}_{cur} <$ Max PDR_{max}))
5. Forward the Data Packet
6. Else
7. Inform source node malicious behavior of node 'i'
8. End

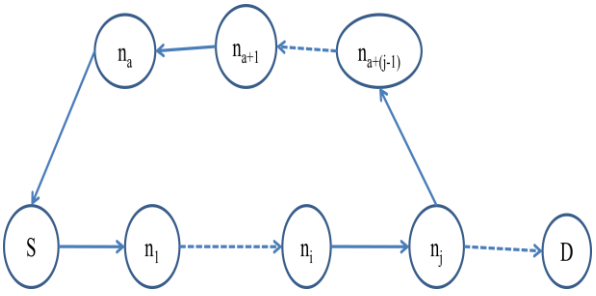

FIGURE 1: Communicating Node Failures

After identifying the malicious node from the above algorithm, n_j that is immediate neighbor of malicious node communicates about the malicious node to the sender node through an alternate path. This is diagrammatically shown as below figure 1. In the diagram S is the sender node, D is the destination node n_i and n_j are intermediate node, where n_i is the malicious node. Alternative path for path between n_i and n_j are through n_a, n_{a+1} and $n_{a+(j-1)}$.

Once the malicious node is found in the figure 1, n_i is the malicious node. Then n_j communicates the identified malicious

node to the sender with an alternative path. Here, present performance evaluation results. Security implemented with R3E using the ns-2 simulator.

4. Results and Discussion

Define the node density as the number of nodes deployed in a 200 m*200 m square area. Around 40 nodes are initialized and used in the paper. One hundred randomly connected topologies for each node. The node transmission range is set to 50 m. The destination node is positioned at bottom left (0 m, 0 m), and the source node is positioned at top right (200 m, 200 m). In order to highlight the potential collision problem between the returning RREP and RREQs, RREP is not acknowledged by the guide nodes at each hop in our simulation. MAC type for proposed method is IEEE 802.11. The performance of the proposed scheme is assessed by using network simulator (ns-2). Using TCL language the paper is being implemented. Here considered type of the traffic is Constant Bit Rate and agent type is UDP. Two ray ground propagation model and using AODV protocol.

4.1 Performance Parameters

Following performance parameters are to be considered to evaluate the effectiveness of proposed mechanism. They are;

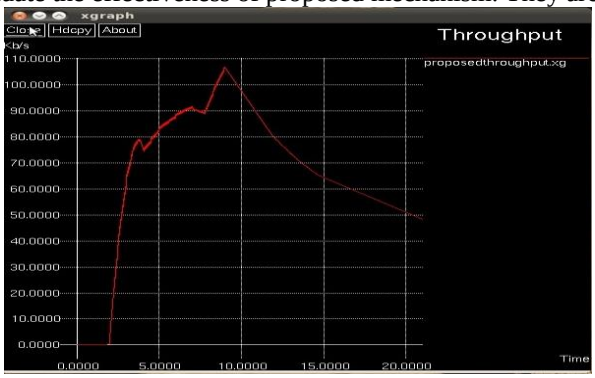

FIGURE 2: THROUGHPUT

Throughput is the average rate of accomplished message convey over a correspondence channel. The throughput is for the most part measured in bits consistently (bit/s or bps). Throughput is measure of information got by the collector. Figure 2 shows the throughput that is, bits transmitted (Kilo-bit/s or Kbps) is plotted in Y-axis. Time taken for transmission is plotted in X-axis. Initially when data packets are sent between the nodes bits transmitted are pretty high, hence graph then shows peak. Gradually when packets of data are transmitting slows down, then graph becomes almost stable and settle down because of less in transmission of bits over that time.

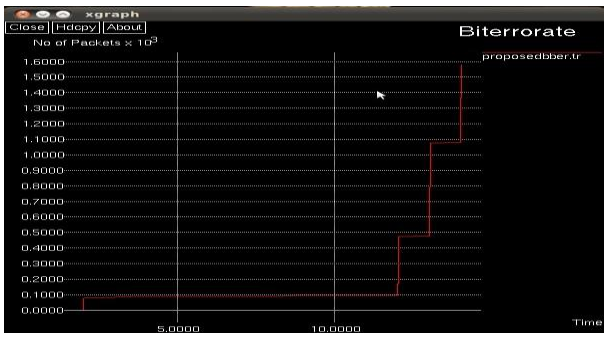

FIGURE 3: BIT-ERROR-RATE

In digital transmission, the number of bit errors is the number of received bits of a data stream over a communication channel that has been altered due to noise, inference, distortion or bit synchronization error. Figure 3 shows the bit-error rate that is number of packets transmitted is plotted in Y-axis. Time taken for transmission of packets is plotted in X-axis. Initially when data packets are transmitting there exist some number of bit-error rate in the system. This thereafter attains a state which is almost stable in condition. And this increases gradually, because of increase in bit-error in the system over that time.

FIGURE 4: PACKET DELIVERY RATIO

Packet Delivery Ratio is the ratio of actual packet delivered to total packets. One or many packets communicating but it fail to meet destination is known as packet drop or loss. Figure 4 show the packet delivery ratio that is; the proportion of receiving and sending of packet is plotted in the Y-axis as PDR. Time taken for transmission of packets is plotted in X-axis. Initially packets sent and received are more hence the proportion of PDR is high as plotted in the graph. Then after this, there happens only some transmission of packets and hence graph stabilizes as shown in graph.

FIGURE 5: CONTROL OVERHEAD PACKETS

I can be achieve trusted communication of the data, when it sending the control or outstanding data. Figure 5 shows the control over-head that is, number of packets transmitted is plotted in Y-axis. Time taken for transmission of packets is plotted in X-axis. Initially number of packets transmitted increases gradually, hence the control over-head of the system increases with it. During certain time, there is almost only little number of packets transmitting hence during which graph shows stable. After this, control over-head increases due to increase in number of packets of data.

5. Conclusion

The section discusses about the conclusion and future work of the paper. Discussion is on conclusion of the R3E along with enhancement of the same. In the work, presenting security, which can incorporate most existing reactive routing protocols in WSNs/IWSNs to provide reliable and efficient packet delivery along with the security. Back-off scheme in the route discovery phase to find a robust virtual path with low overhead. Without utilizing the location information, data packets can still be greedily progressed toward the destination along the virtual path. Therefore, R3E provides very close routing performance to the geographic opportunistic routing protocol. With this reactive routing with security is like a boon to the wireless network. Security from the nodes trying to modify the data while data transmission. Based on the threshold value range malicious node is found. Removing them on when acknowledged in the network, will improves the reliability of the network still more than that of R3E.

Reference

[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] 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.

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

[7] Sajal K. Das ,JianweiNiu, Long Cheng, Yu Gu and Lei Shu, " Reliable Reactive Routing Enhancement of Wireless Sensor Network ," on May 2013

[8] 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.

[9] 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.

[10] F. Barac, J. Akerberg, and M. Gidlund, "A lightweight routing protocol for industrial wireless sensor and actuator networks," in Proc. IECON, 2011, pp. 2980–2985.

[11] K. Yu, M. Gidlund, J. Åkerberg, and M. Björkman, "U. D. of Energy, Industrial wireless technology for the 21st century," in Proc. IECON, 2012, pp.

[12] K. Zeng, W. Lou, J.Yang, and D. Brown, "On geographic collaborative forwarding in wireless ad hoc and sensor networks," in Proc. WASA, 2007, pp. 11–18.

[13] Sajal K. Das ,JianweiNiu, Long Cheng, Yu Gu and Lei Shu, " Reliable Reactive Routing Enhancement of Wireless Sensor Network ," on May 2013.

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

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

[16] E. Royer and C.-K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," *IEEE Pers. Commun.*, vol. 6, no. 2, pp.46–55, 1999.

[17] R. Shah, S. Wietholter, A. Wolisz, and J. Rabaey, "When does opportunistic routing make sense?," in *Proc. IEEE PerCom Workshops*, 2005, pp. 350–356.

Author's Profile

Akash Joshi, Completed B.E with Information Science & Engineering in Basaveshwara Engineering College (BEC), Bagalkot & pursuing M.Tech with Computer Science & Engineering in VTU-Centre for PG Studies, VIAT, Muddenahalli, Bengaluru Region, India.

Dr. Shiva Murthy G completed B.E(CSE) and M.E(CSE) from Bangalore University. He Received Ph.D from National Institute of Technology Karnataka (NITK). He has published his publications IEEE Journals Currently he is working as Associate Professor and Head, Dept of MCA, VTU Center for PG Studies, Bangalore Region, Muddenahalli.