Review Paper on Reliability and Lifetime Optimization in Wireless Sensor Network

Rashmi D. Gaikwad
M. Tech Scholar
B.I.T. Ballarpur, Chandrapur
rashmigaikwad1307@gmail.com

Prof. Sagar Bhakre
Assistant Professor
B.I.T. Ballarpur, Chandrapur
bhakresagar@gmail.com

Abstract: A wireless sensor network (WSN) is a computer network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations.[1] The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control.[1]

*****

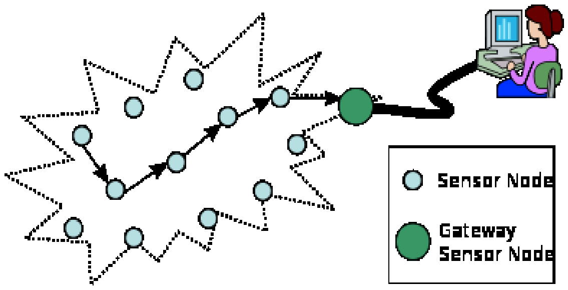
I. INTRODUCTION

Wireless sensor networks (WSNs) are typically composed of hundreds to thousands of small collaborating wireless sensor nodes. The development of WSN has received increasing attention from various industries. The main task of a wireless sensor network is to monitor the area concerned, collect data and transmit the data to the sink node. Sink node makes the decision based on the collected data from one or more source nodes. In wireless sensor networks, sensors are usually deployed in some harsh environment by aircrafts in order to achieve the specific quality of service. Sensors have only limited battery energy and communication capacities while they need to work for a long time. One essential requirement for sensor networks is the reliability of applications.[2] A key functionality of WSNs consists in obtaining and transporting the information of interest (e.g.,events/status) required by the different applications having varied requirements on the reliability and timeliness of data delivery. While node redundancy, inherent in WSNs, increases the fault tolerance, no guarantees on reliability levels can be assured.

Source nodes: which generate data, usually by using sensors to measure environmental factors such as temperature, humidity or radiation,

Sink nodes: which collect the data gathered by source nodes and

Intermediate nodes: which may include source nodes that aid the transmission from source to sink.



Characteristics

Unique characteristics of a WSN are:

- Small-scale sensor nodes
- Limited power they can harvest or store
- Harsh environmental conditions
- Node failures
- Mobility of nodes
- Dynamic network topology
- Communication failures
- Heterogeneity of nodes
- Large scale of deployment
- Unattended operation

Reliability

Reliability is a big barrier for WSN to be commercialized. A wireless link is generally felt to be unreliable compared to wire. Due to attenuation, shadowing and interference, a packet transmitted on a wireless link can be lost. Since WSNs may be deployed in a harsh environment and operates in the industrial, scientific and medical (ISM) band, they are prone to the above problems. The last but not the least, the imperfect hardware may also cause unreliability. By imperfection we do not mean malfunction of hardware.

Instead we mean the problem arisen due to the low cost hardware which cannot be miniaturized without compromising on some precisions. For example, clocks on the devices may drift with time; the coverage of antennas on these devices is far from Omni-directional, thus a common assumption of Omni-directional antenna beam in WSN research is not valid anymore. This challenge has to be addressed when designing a WSN protocol.

Energy

In WSNs, since devices are left untouched the energy consumption need to be taken into account. While the number of transistor on a chip doubling every 18-24 months, according to Moore's law, the energy capacity in a battery only increases 8-10% per year and this trend is continuing. It means that instead of two year, the battery energy capacity doubles every 10 years. This mismatch is driving researchers to explore how to extend the lifetime of WSNs.

Scalability

A WSN may contain only a few nodes or hundreds of node. An event may be tracked with a frequency of once per day or once per second. An event may be reported only by a single node or by many nodes simultaneously. In the latter cases, scalability of the WSN is challenged. Since the devices operate in the same frequency, transmissions from different nodes may contend with each other or even collide. Applications such as fire monitoring cannot tolerate consequences of the contention and collision, either delay or miss of detection leads to great damage. Since links suffer from contentions or collisions, routes can be unreliable due link variability. Researchers have been trying to select relatively more reliable links to build up a route. Although contentions and collisions in a large network can be alleviated by an advanced scheduling protocol, which coordinates node to access the medium at different times, more solutions are available. For instance, we can reduce transmission power of nodes so that less contentions are expected; nodes can also gather into groups, e.g. clusters, where only a head of the cluster participates in routing or management traffic, so that less traffic is generated and contentions and collisions are reduced.

II. EXISTING SYSTEM

In Geographic and energy aware routing (GEAR), the sink node disseminates requests with geographic attributes to the target region instead of using flooding. Each node forwards messages to its neighboring nodes based on estimated cost and learning cost. Source-location privacy is provided through broadcasting that mixes valid messages with dummy messages. The transmission of dummy messages not only consumes significant amount of sensor energy, but also increases the network collisions and decreases the packet delivery ratio. In phantom routing protocol, each message is routed from the actual source to a phantom source along a designed directed walk through either sector based approach or hop-based approach. The direction/sector information is stored in the header of the message. In this way, the phantom source can be away from the actual source. Unfortunately, once the message is captured on the random walk path, the adversaries are able to get the direction/sector information stored in the header of the message.

Disadvantages Of Existing System

- More energy consumption
- Increase the network collision
- Reduce the packet delivery ratio

III. PROPOSED SYSTEM

We propose a secure and efficient Cost Aware Secure Routing (CASER) protocol that can address energy balance and routing security concurrently in WSNs. In CASER routing protocol, each sensor node needs to maintain the energy levels of its immediate adjacent neighboring grids in addition to their relative locations. Using this information, each sensor node can create varying filters based on the expected design tradeoff between security and efficiency. The quantitative security analysis demonstrates the proposed algorithm can protect the source location information from the adversaries. In this project, we will focus on two routing strategies for message forwarding: shortest path message forwarding, and secure message forwarding through random walking to create routing path unpredictability for source privacy and jamming prevention.

Advantages of Proposed System

- Reduce the energy consumption
- Provide the more secure for packet and also routing
- Increase the message delivery ratio
- Reduce the time delay

Applications

The applications for WSNs are many and varied. They are used in commercial and industrial applications to monitor data that would be difficult or expensive to monitor using wired sensors. They could be deployed in wilderness areas, where they would remain for many years (monitoring some environmental variable) without the need to recharge/replace their power supplies. They could form a perimeter about a property and monitor the progression of intruders (passing information from one node to the next). There are a many uses for WSNs.

Typical applications of WSNs include monitoring, tracking, and controlling. Some of the specific applications are habitat monitoring, object tracking, nuclear reactor controlling, fire detection, traffic monitoring, etc. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes.

- Environmental monitoring
- Habitat monitoring
- Military surveillance
- Inventory tracking
- Medical monitoring
- Smart spaces
- Process Monitoring

IV. CONCLUSION

Poles apart WSN applications necessitate unusual positions of reliability. Communication protocols for WSN should be reliable and energy-efficient to keep away from unproductive stabbing of energy resources through minimization of control and retransmission overhead.In this paper,WSN reliability research fields are discussed.Future directions and technical challenges are proposed. These objectives can be obtainted by developing the efficient mechanism for clustering the sensor nodes in heterogeneous WSNs. We can have cluster based efficient data aggregation technique which considers both energy and reliability.

REFRENCES

[1] Y. Li, J. Ren, and J. Wu, “Quantitative measurement and design of source-location privacy schemes for wireless sensor networks,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 7, pp. 1302–1311, Jul. 2012.

[2] Y. Li, J. Li, J. Ren, and J. Wu, “Providing hop-by-hop authentication and source privacy in wireless sensor networks,” in Proc. IEEE Conf. Comput. Commun. Mini-Conf., Orlando, FL, USA, Mar. 2012, pp. 3071–3075.

[3] B. Karp and H. T. Kung, “GPSR: Greedy perimeter stateless routing for wireless networks,” in Proc. 6th Annu. Int. Conf. Mobile Comput.Netw. New York, NY, USA, 2000, pp. 243–254.

[4] J. Li, J. Jannotti, D. S. J. De Couto, D. R. Karger, and R. Morris, “A scalable location service for geographic ad hoc routing,” in Proc. 6th Annu. Int. Conf. Mobile Comput.Netw, 2000, pp. 120–130.

[5] Y. Xu, J. Heidemann, and D. Estrin, “Geography-informed energy conservation for ad-hoc routing,” in Proc. 7th Annu. ACM/IEEE Int. Conf. Mobile Comput.Netw., 2001, pp. 70–84.

[6] Y. Yu, R. Govindan, and D. Estrin, “Geographical and energyaware routing: A recursive data dissemination protocol for wireless sensor networks,” Comput. Sci. Dept., UCLA, TR-010023, Los Angeles, CA, USA, Tech. Rep., May 2001.

[7] N. Bulusu, J. Heidemann, and D. Estrin, “GPS-less low cost outdoo localization for very small devices,” Comput. Sci. Dept., Univ. Southern California, Los Angeles, CA, USA, Tech. Rep. 00- 729, Apr. 2000.

[8] A. Savvides, C.-C.Han, and M. B. Srivastava, “Dynamic finegrained localization in ad-hoc networks of sensors,” in Proc. 7th ACM Annu.Int. Conf. Mobile Comput.Netw., Jul. 2001, pp. 166–179.

[9] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, “Routing with guaranteed delivery in ad hoc wireless networks,” in Proc. 3rd Int. Workshop Discrete Algorithms Methods Mobile Comput. Commun., 1999, pp. 48–55.

[10] Y. Li, Y. Yang, and X. Lu, “Rules of designing routing metrics for greedy, face, and combined greedy-face routing,” IEEE Trans. Mobile Comput., vol. 9, no. 4, pp. 582–595, Apr. 2010.

[11] R. Shah and J. Rabaey, “Energy aware routing for low energy ad hoc sensor networks,” in Proc. IEEE Wireless Commun. Netw.Conf.,Mar. 17–21, 2002, vol. 1, pp. 350–355.

[12] J.-H. Chang and L. Tassiulas, “Maximum lifetime routing in wireless sensor networks,” IEEE/ACM Trans. Netw., vol. 12, no.4, pp. 609–619, Aug. 2004.