SURVEY ON SLEEP SCHEDULING METHODS IN WIRELESS SENSOR NETWORKS

S. Kousalya Devi, II-M.E, Erode Sengunthar Engineering College, Erode

Mrs.C.Kavitha, Assistant Professor (SLG-1), Erode Sengunthar Engineering College, Erode

***ABSTRACT**:* In most WSN applications, the overall traffic profile is very simple as packets only Flow from sensor nodes to the data sinks and vice versa, with very few inter-node exchanges. Despite this simplicity in traffic flows, the WSN is still expected to deliver Sensor data and network control messages with high fidelity in a timely fashion. Aside from packet loss effects presiding over unstable wireless links, the inherent multihop Nature of WSN communications present additional uncertainty in guaranteeing packet transport reliability that the common protocols used in the Internet paradigm are inadequate to handle. In particular, it remains a considerable challenge to preserve the network connectivity in conjunction with low-duty cycles leap-scheduling strategies intended for maximum energy conservation.

Index terms: Sensor node, Multihop, Data sink, Leap-scheduling

I INTRODUCTION

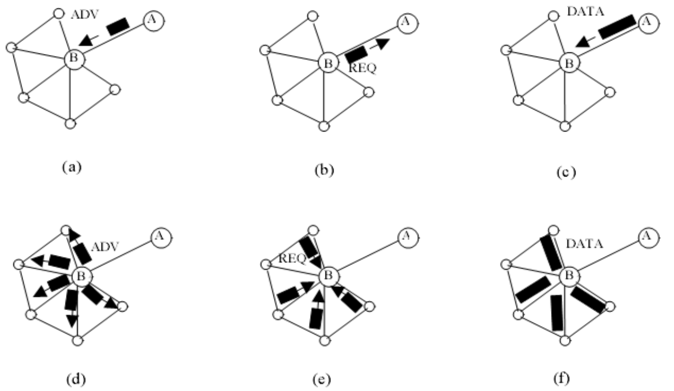
Wireless Sensor Network (WSN) is a collection of spatially deployed wireless sensors by which to monitor various changes of environmental conditions (e.g., forest fire, air pollutant concentration, and object moving) in a collaborative manner without relying on any underlying infrastructure support. Recently, a number of research efforts have been made to develop sensor hardware and network architectures in order to effectively deploy WSNs for a variety of applications. Due to a wide diversity of WSN application requirements, however, a general-Purpose WSN design cannot fulfill the needs of all applications. Many network parameters such as sensing range, transmission range, and node density have to be carefully considered at the network design stage, according to specific applications.

To achieve this, it is critical to capture the impacts of network parameters on network performance with respect to application specifications. Wireless sensor networks are deployed to monitor the sensing field and gather information from it. Traditionally, two approaches can be adopted to accomplish the data collection task: through direct communication, and through multi-hop forwarding. In the first case, sensor nodes upload data directly to the sink through one-hop wireless communication, which may result in long communication Distances and degrade the energy efficiency of sensor nodes. On the other hand, with multi-hop forwarding, data are reported to the sink through multiple relays, and the communication distance is reduced. However, since nodes near the sink generally have a much heavier forwarding load,

Their energy may be depleted very fast, which degrades the network performance

II ROUTING

When a node desires to transmit, it captures the token and attaches the message. As the token passes, the destination reads the header, and captures the message. In some schemes, it attaches a 'message received' signal to the token, which is then received by the original source node. Then, the token is released and can accept further messages. The token ring is a completely decentralized scheme that effectively uses TDMA.



Protocol Design

Fixed routing schemes often use Routing Tables that dictate the next node to be routed to, given the current message location and the destination node. Routing tables can be very large for large networks, and cannot take into account real-time effects such as failed links, nodes with backed up queues, or congested links.

Adaptive routing schemes depend on the current network status and can take into account various performance measures, including cost of transmission over a given link, congestion of a given link, reliability of a path, and time of transmission. They can also account for link or node failures.

ROUTING PROTOCOL

Routing has two main functions: route discovery and packet forwarding. The former is concerned with discovering routes between nodes, whereas the latter is about sending data packets through the previously discovered routes. There are different types of ad hoc routing protocols. One can distinguish proactive and reactive protocols. Protocols of the latter category are also called on-demand protocols. Another type of classification distinguishes routing table based protocols (e.g., DSDV) and source routing protocols (e.g., DSR).

REQUIREMENTS OF ROUTING

The major requirements of a routing protocol

- Minimum route acquisition delay
- Quick route reconfiguration in the case of path breaks.
- Loop-free routing
- Distributed routing protocol
- Low control over-head
- Scalability with network size
- QoS support as demanded by the application
- Support of time-sensitive traffic

III NATURES OF ROUTING

Nodes exchange routing information periodically in order to maintain consistent and accurate information.

- To transmit data to a destination, path can be computed rapidly based on the updated information available in the routing table.
- The disadvantage of using a proactive protocol is high overhead needed to dynamic topology that might require a large number of routing updates.
- Each node maintains a routing table, with an entry for each possible destination address, next hop on the shortest path to that destination, shortest known distance to this destination, and a destination sequence number that is created by the destination itself.

Reactive Routing Protocols (On-demand)

Route discovery mechanism is initiated only when a node does not know the path to a destination it wants to communicate with.

In case of mobile ad hoc network, reactive routing protocols have been demonstrated to perform better with significantly lower changes that may occur in node connectivity, and yet are able to reduce/eliminate routing overhead in periods or areas of the network in which changes are less frequent.

A reactive routing has two main operations. Route discovery (usually broadcasting using a form of controlled flooding) and route maintenance. Various reactive protocols have been proposed in literature such as Ad Hoc On-demand vector (AODV), Dynamic source routing (DSR), Temporary Ordered Routing Algorithm (TORA).

IV RELATED WORKS

The description of some works related to the sleep scheduling and energy consumption method is given in this section.

Sleep Wake Scheduling

Measurements have shown that the energy that a sensor node spends while idly listening amounts to 50%-100% of the energy required for receiving. Furthermore, typically, a sensor node would spend a substantial fraction of the time in the idle state. Therefore, idle listening has been recognized as one of major sources of energy waste in sensor networks and sleep scheduling has been widely studied. The mainstream of research on sleep scheduling can be divided into two approaches. One approach, the "periodical packet-arrival based approach", assumes periodical packet arrival, thus proposing a periodic active/sleep (i.e., ON/OFF) schedule. The second approach is "coverage-based approach", which assumes large density of sensor nodes, thus maintaining the connectivity of the network by a subset of nodes which are ON all the time, while letting the other nodes sleep. There are also various strategies for adaptation of the sleeping schedule, that is ending the ON period according to different criteria, such as the overheard messages, the network topology, the residual energy of the nodes, the most recently updated neighbor sleeping schedule, the database of neighbor nodes' sleeping schedule, the number of packets queued in the MAC layer, and the waiting time of packets and the length of waiting queue in the previous node.

Energy-Quality Tradeoffs for Target Tracking in Wireless Sensor Networks

The tradeoffs involved in the energy-efficient localization and tracking of mobile targets by a wireless sensor network. The framework for evaluating the fundamental performance of tracking strategies in which only a small portion of the network is activated at any point in time. First compare naive network operation with random activation and selective activation. In these strategies the gains in energy-savings come at the expense of increased uncertainty in the location of the target, resulting in reduced quality of tracking. The selective activation with a good prediction algorithm is a dominating strategy that can yield orders-of-magnitude energy savings with negligible difference in tracking quality, then consider duty-cycled activation and show that it offers a flexible and dynamic tradeoff between energy expenditure and tracking error when used in conjunction with selective activation. There is an emerging trend towards the use of sophisticated wireless networks of unattended sensor devices for intelligence gathering and environmental monitoring. One \ canonical application of sensor networks that has received considerable attention in the literature is the tracking of a mobile target (point source) by the network. In a tracking scenario, information obtained from nodes far away from the region of activity is of little or no use. For a typical sensor network with a large number of nodes, a major portion of these falls in the above category. In addition, if the nodes are densely deployed information obtained from some sensors close to the region of activity might be redundant. An obvious way to save energy is to switch on only a subset of the sensor nodes. There are various possible activation strategies: (1) naive activation, (2) randomized activation (3) selective activation based on trajectory prediction and (4) duty-cycled activation. In these sensor activation strategies, energy savings come at the expense of a reduction in the quality of tracking. In other words, relying on the information provided by a small subset of the sensor nodes results in an increased uncertainty in the sensed location of the mobile. The energy-quality tradeoffs involved by building a model to quantify both the energy expenditure and the quality of tracking. Also for a particular strategy, the impacts are: a) deployed/activated density of sensors b) their sensing range c) capabilities of activated and un-activated nodes d) the target's mobility model.

It is not directed *per se* at proposing new techniques for mobile tracking. Rather the focus is on the evaluation and analysis of general strategies which may be incorporated into a real system. Start with a simple model for tracking and substantiate the intuition that it is possible to obtain orders of magnitude savings in energy while keeping the uncertainty within acceptable limits and the extensions of the model to relate closely with real life scenarios. The results in this work are a first step, attempt to understand the fundamental bounds on the the tracking quality that can be obtained under various energy constraints and sensor models.

DCTC: Dynamic Convoy Tree-Based Collaboration For Target Tracking In Sensor Networks

Most existing work on sensor networks concentrates on finding efficient ways to forward data from the information source to the data centers, and not much work has been done on collecting local data and generating the data report. The proposing techniques to detect and track a mobile target. A new concept of dynamic convoy tree-based collaboration, and formalize it as a multiple objective optimization problem which needs to find a convoy tree sequence with high tree coverage and low energy consumption. The proposed scheme is an optimal solution which achieves 100% coverage and minimizes the energy consumption under certain ideal situations. Considering the real constraints of a sensor network, several practical implementations: the conservative scheme and the prediction-based scheme for tree expansion and pruning; the sequential and the localized reconfiguration schemes for tree reconfiguration. Extensive experiments are conducted to compare the practical implementations and the optimal solution. The results show that the prediction-based scheme outperforms the conservative scheme and it can achieve similar coverage and energy consumption to the optimal solution. The experiments also show that the localized reconfiguration scheme outperforms the sequential reconfiguration scheme when the node density is high, and the trend is reversed when the node density is low. Most existing researches in sensor networks, e.g., the directed diffusion, LEACH, and two-tier data dissemination (TTDD), concentrate on finding efficient ways to forward the data report to the data center, and not much work has been done on how to detect the mobile target and generate robust and reliable reports in an energy efficient way. Recently, Chu et al. studied the problem of tracking a mobile target using an information-driven approach. However, their approach assumed that a single node close to a target can detect the status of the target, and did not consider the collaboration among nodes that can detect the target at the same time. Since sensor nodes deployed in current sensor networks do not have a large sensing distance, or a high level of sensing accuracy and node reliability, Cerpa et al suggested that multiple nodes surrounding the target should collaborate to make the collected information more complete, reliable, and accurate. However, no concrete algorithm was given.

A big challenge of implementing the DCTC framework is how to reconfigure the convoy tree in an energy efficient way as the target moves. To address this problem, First formalize it as an optimization problem of finding a min-cost convoy tree sequence with high tree coverage, and give an optimal solution (o-DCTC) based on dynamic programming. Considering the constraints of sensor networks and practical solutions. Specifically, propose two tree expansion and pruning schemes: the conservative scheme and the prediction- based scheme; and two tree reconfiguration schemes: the sequential reconfiguration and the localized reconfiguration, also evaluate the performance of the optimal solution and the practical implementations through extensive simulations. Based on the simulation results, when the same reconfiguration scheme is used, the prediction-based scheme outperforms the conservative scheme and it can achieve a similar coverage and energy consumption to the optimal solution. When using the same scheme for tree expansion and pruning, the localized reconfiguration scheme outperforms the sequential reconfiguration scheme when the node density is high, and the trend is reversed when the node density is low.

Monitoring Of Wireless Sensor Networks

In wireless sensor networks, services may fail due to various reasons, including radio interference, de-synchronization, battery exhaustion, or dislocation. Such failures are caused by software and hardware faults, environmental conditions, malicious behavior, or bad timing of a legitimate action. In general, the consequence of such an event is that a node becomes unreachable or violates certain conditions that are essential for providing a service, for example by moving to a different location, the node can no further provide sensor data about its former location. In some cases, a failure caused by a simple software bug can be propagated to become a massive failure of the sensor network. This results in application trials failing completely and is not acceptable in safety critical applications. The open nature of the wireless communication, the lack of infrastructure, the fast deployment practices, and the hostile deployment environments, make them vulnerable to a wide range of intrusions and security attacks. The motivation for attacking a sensor networks could be, for example, to gain an undeserved and exclusive access to the collected data. There has been a multitude of attacks described in the literature: probabilistic data packet dropping, topology manipulation, routing table manipulation, prioritized data and control packet forwarding, identity falsification, medium access selfishness etc. The protection system of a sensor networks usually relies on the following two mechanisms:

(i) Authentication and secure protocols and (ii) intrusion and attack (misbehavior) detection. As the experience from the Internet shows, the weaknesses in authentication and secure protocols are frequently exploited. These protocols alone are in general considered being insufficient to provide the necessary level of protection. Therefore, there has been a lot of effort invested in providing networks with means for a timely detection of an attack or intrusion. Such detection is often based on methods and algorithms known from the field of machine learning. Additionally, After sensors get deployed in the monitored area, the access to them can be difficult. For example, a sensor network, with the goal to monitor conditions in the sewer system of a large city, might be inaccessible for maintenance, software updates or battery exchange. Therefore, a special focus has been put on designing energy efficient protocols at all layers of the OSI (Open Systems Interconnection protocol stack. Additionally to addressing energy constraints, these protocols should impose a high degree of robustness in order to minimize the need for human intervention. The use of these sensor networks in hostile environments means that providing quality of service is essential and requires the implementation of fault-tolerant mechanisms that can ensure availability and continuity of service. For example, the maximum coverage of the regions monitored by the network and connectivity of the various nodes of the network must be maintained. However in an environment where each node can fail unexpectedly resulting in the isolation of some parts of the network, this guarantee is neither automatic nor easy to achieve. For all this problems, the integration of mechanisms for monitoring wireless sensor networks, for the reason of topology control, fault tolerance and security are crucial for the effective use of wireless sensor networks. There are many current management approaches, but each provides only partial solutions to the problems of monitoring and fault tolerance, and they do not adapt to the properties and constraints of many wireless sensor networks.

Monitoring Of Connectivity and Coverage in WSN

Connectivity is particularly important for wireless sensor networks. In a wireless sensor network, the deployment strategy often involves using more nodes then necessary and turning off the ones that are not being used for communication or sensing. When the network becomes disconnected, one or more of the redundant nodes can be turned on to repair connectivity. The main problem with this technique is the requirement for extra nodes, and when several nodes in a limited region fail it may no longer be possible to repair the network. The problem of adding as few nodes as possible to a disconnected static network so that the network remains connected. They show that the problem is NP-Complete and propose some heuristic solutions. These algorithms require global knowledge of the graph and they are time-consuming to apply. Consequently they are typically not applicable in real-time with dynamic networks. Using mobility to maintain connectivity has attracted many researchers. The general approach has been the use of mobility to carry data between disconnected components of the network. Another approach is the storage of data when connectivity is disrupted, and sending the data when connectivity is subsequently repaired. A significant problem with these approaches is the latency in data transfer for time critical applications. There are also approaches that can be used to maintain uninterrupted connectivity with dynamic networks. Proposed technique for providing radio connectivity while moving a group of robots from one configuration to another. However, this analysis is not valid when there are obstacles. Several other solutions for fault tolerance are based on the nature of redundant sensor networks. Fusion techniques may merge or aggregate the different readings of the sensors. Multi routing paths and techniques to ensure k-connectivity between nodes can be applied to increase the reliability of the transmission of messages in wireless sensors networks.

Critical Event Monitoring In Wireless Sensor Networks

Local monitoring is a collaborative detection strategy where a node monitors the control traffic going in and out of its neighbors.. Many techniques have been introduced that use the framework of local monitoring to achieve specific tasks such as intrusion detection, building trust and reputation among nodes, protecting against control and data traffic attacks, and building secure routing protocols. Though local monitoring has been demonstrated as a powerful technique for enhancing security of WSNs, it results in a high energy cost since it requires the monitoring nodes to be constantly awake to oversee network activity, partially addressed the problem of combining local monitoring (to support security) and sleep-wake scheduling (to conserve energy) under the assumption that a malicious node does not have the ability to control its transmission power level. Another limitation is that not consider scheduling of the monitoring nodes with the goal of additional energy savings.

Obviously, sleep scheduling could cause transmission delay because sender nodes should wait until receiver nodes are active and ready to receive the message. The delay could be significant as the network scale increases. Therefore, a delay-efficient sleep scheduling method needs to be designed to ensure low broadcasting delay from any node in the WSN. Recently, many sleep schedules for event monitoring have been designed. However, most of them focus on minimizing the energy consumption. Actually, in the critical event monitoring, only a small number of packets need to be transmitted during most of the time. When a critical event is detected, the alarm packet should be broadcast to the entire network as soon as possible. Therefore, broadcasting delay is an important issue for the application of the critical event monitoring. To minimize the broadcasting delay, it is needed to minimize the time wasted for waiting during the broadcasting. Finally, the transmission failure due to some unreliable wireless links may cause the retransmission during the next duty cycle, which also results in large delay equaling the whole duty cycle.

V COMPARATIVE STUDY

Sleep scheduling methods	Advantages	Energy Consumption
Coverage Based Approach	Large density	50%-60%
Trajectory Prediction	Flexible Energy Saving	55%-60%
Tree Expansion Tree pruning	Accuracy Reliability	57%-62%
Intrusion Attack Detection	Security Fast Deployment	60%-66%
NP Complete Graph Theory	Time Consuming Data Secure	65%-71%
Novel Scheme	Low Broadcasting delay	65%-77%
Local Monitoring	Energy Consumption Throughput	75%-79%

VI CONCLUSION

Owing to large-scale availability of low-cost sensors, sensors are often deployed with some redundancy; that is, several locations in the target field can be monitored by multiple sensors. Lifetime of the WSNs can be substantially enhanced by intelligently activating the sensors that monitor the target field at any given time. Then seek to maximize the lifetime of sensor networks by designing algorithms that dynamically activate sensors based on their residual energy content. The Sleep scheduling algorithm is developed completely distributed, does not need to know the coordinates of any sensor, and provides provable guarantees on the attained lifetimes.

REFERENCES

[1] Ateniese.G, Burns.R.C, Curtmola.R, Herring.J, Kissner.L, Peterson.Z.N.J, and Song. D.X (2007), “Provable data possession at untrusted stores,” in ACM Conference on Computer and Communications Security.

[2] Ateniese.G, Pietro.R.D, Mancini.L.V, and Tsudik.G (2008), “Scalable and efficient provable data possession,” in Proceedings of the 4th international conference on Security and privacy in communication networks, Secure Comm.

[3] Brownfield.M.I, Davis.N.J, Fayez.A.S, Mehrjoo.K, (2011) “Monitoring Of Wireless Sensor Networks” in IEEE Conference on the 7th International Conference on Collaborative Computing, October 15-18.

[4] Cong Wang, Qian Wang, and Kui Ren (2009), “Ensuring Data Storage Security in Mobile Computing”, international workshop on QoS.

[5] Dodis.Y, Vadhan.S.P, and Wichs.D (2009), “Proofs of retrievability via hardnes amplification,” in ser. Lecture Notes in Computer Science, vol.5444.

[6] Du.S, Gurewitz.O, Johnson.D.B, Sun.Y (2011) “Sleep Wake Scheduling” in ACM Conference on Computer and Communications Security

[7] Erway.C.C, Kupcu.A, Papamanthou.C, and Tamassia.R(2009), “Dynamic provable data possession,” in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM.

[8] Fortnow.L, Rompel.J, and Sipser.M (1988), “On the power of multiprover interactive protocols,” in Theoretical Computer Science.

[9] Juels.A and Kalisk.B (2007), “Pors: proofs of retrievability for large files,” in ACM Conference on Computer and Communications Security.

[10] Mehul A. Shah Ram Swaminathan Mary Baker (2008),”Privacy-Preserving Audit and Extraction of Digital Contents”.

[11] Insang Song, Jeewoong O.K, Juryon Paik, Seung-Cheol Lee (2011) “Monitoring Of Connectivity and Coverage in WSN” ,” in ACM Conference on Computer and Communications Security.

[12] Shacham.H and Waters.B (2008), “Compact proofs of retrievability,” in ASIACRYPT, ser.Lecture Notes in Computer Science, Ed., vol. 5350.