An Energy Efficient Cluster based Load Balance Routing for Wireless Sensor Network

K. Karthika[1] Ms. D. Vetrithangam[2]
[1]M. E. (Final year) [2]M. E. & Ph. D
[2]Assistant Professor
[1, 2]RatnaVel Subramaniam College of Engineering & Technology.

Abstract--- Redundancy management of heterogeneous wireless sensor networks, utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes. The concept of redundancy management is to exploit the tradeoff between energy consumption vs. the gain in reliability, timeliness, and security to maximize the system useful lifetime. Formulate an optimization problem for dynamically determining the best redundancy level to apply multipath routing for intrusion tolerance. A voting-based distributed intrusion detection algorithm is applied to detect and evict malicious nodes. Develop a novel probability model to analyze the best redundancy level in terms of path redundancy and source redundancy, as well as the best intrusion detection settings in terms of the number of voter sand the intrusion invocation interval under which the lifetime of network is maximized. The coverage time for a clustered wireless sensor network by optimal balancing of power consumption among cluster heads. Clustering significantly reduces the energy consumption of individual sensors, but it also increases the communication burden on CHs. Two mechanisms are proposed for achieving balanced power consumption in the stochastic case: a routing-aware optimal cluster planning and a clustering-aware optimal random relay. A sleeping node mechanism is used in order to gain maximum energy.

Keywords: Heterogeneous wireless sensor networks, multipath routing, intrusion detection, reliability, security, energy conservation.

I. INTRODUCTION

A wireless sensor network (shortly WSN) consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance. They are now used in many industrial and civilian application areas, including industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and traffic control. In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery.

A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few pennies, depending on the size of the sensor network and the complexity required of individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth.

The multipath routing for intrusion tolerance query response success probability is maximized while prolonging the useful lifetime.

This optimization problem for the case in which a voting-based distributed intrusion detection algorithm is applied to detect and evict malicious nodes in a HWSN. A novel probability model to analyze the best redundancy level in terms of path redundancy and source redundancy, as well as the best intrusion detection settings in terms of the number of voters and the intrusion invocation interval under which the lifetime of a HWSN is maximized.

A unifying metric that considers the above two design tradeoffs, define the total number of queries the system can answer correctly until it fails as the lifetime or the mean time to failure (shortly MTTF) of the system, which can be translated into the actual system lifetime span given the query arrival rate. Aim is to find both the optimal redundancy levels and IDS settings under which the MTTF is maximized, when a given set of parameters characterizing the operational and environment conditions. The coverage time for a clustered wireless sensor network by optimal balancing of power consumption among cluster heads (shortly CHs). Clustering significantly reduces the energy consumption of individual sensors, but it also increases the communication burden on CHs. To investigate this tradeoff, an analytical model incorporates both intra-and inters cluster traffic.

Depending on whether location information is available or not, considers optimization formulations under both deterministic and stochastic setups, using a Rayleigh fading model for inter cluster communications. Each CH routes its traffic directly to the sink or relays it through other CHs. A coverage-time-optimal joint clustering or routing algorithm, in which the optimal clustering and routing parameters are computed using a linear program. A uniformly distributed sensors and provide optimal power allocation strategies that guarantee (in a probabilistic sense) an upper bound on the end-to-end (inter-CH) path reliability. Two mechanisms are proposed for achieving balanced power consumption in the stochastic case: a routing-aware optimal cluster planning and a clustering-aware optimal random relay.

In the first case a clustering approach is developed in the context of shortest hop inter-CH routing. For this scheme, coverage-time maximization is formulated as a binomial optimization problem that is efficiently solved using generalized geometric programming (shortly GGP) techniques. The optimal cluster sizes are obtained from this analysis. In the second case a routing strategy for a given clustering approach e.g., a "load-balanced" clustering, where all clusters are of the same size. According to this approach, a CH probabilistically chooses to relay the traffic to any neighboring "uplink" CH in the direction of the sink. The "optimal" relaying probabilities to various neighbors are derived through linear programming.

The procedure for cluster formation consists of two steps: the deployment of CHs and the assignment of sensors to CHs. Because of the symmetric nature of the area and the uniform distribution of sensors, the formation of clusters is also symmetric, i.e., any two CHs with the same distance to the sink should have the same coverage. Such clusters are said to be of the same type. Suppose there are types of clusters in the network.

II. INDICATION OF THE WSN

Wireless sensor network (shortly WSN) consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance. They are now used in many industrial and civilian application areas, including industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and traffic control.

The cost of sensor nodes is similarly variable, ranging from hundreds of dollars to a few pennies, depending on the size of the sensor network and the complexity required of individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth. A sensor network normally constitutes a wireless ad-hoc network, meaning that each sensor supports a multi-hop routing algorithm.

A. *Appearances of WSN*

- Limited power they can harvest or store
- Ability to withstand harsh environmental conditions
- Ability to cope with node failures Mobility of node
- Dynamic network topology
- Communication failures Heterogeneity of nodes
- Large scale of deployment Unattended operation

Algorithms and protocols need to address the following issues

- Lifetime maximization
- Robustness and fault tolerance
- Self-configuration

B. *Architecture of WSN*

Wireless Sensor Network (shortly WSN) provides a low-cost and multifunctional means to link communications and computer networks to the physical world. It consists of base stations and a number of wireless sensors. Each sensor is a unit with wireless networking capability that can collect and process data independently. Sensors are used to monitor activities of objects in a specific field and transmit the information to the base station.

C. *Sensor node*

This is a mobile node moving freely to monitors the physical environment. Once it detects its physical target, it generates a data packet and sends it to the sink node via the wireless channel. The processor in the sensor node may be set the threshold value to compare with the detected data before it generates and sends a data packet.

D. *Sink node*

This node collects all data packets from sensor nodes and uses them to analyze their targets.

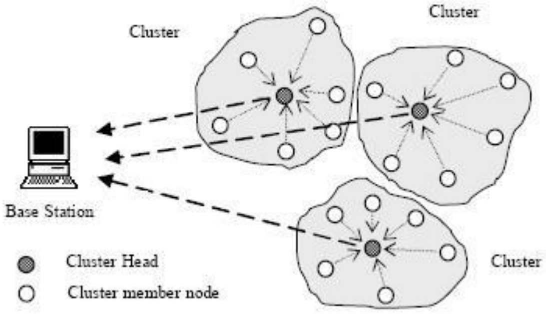

Fig. 1: Architecture of WSN.

E. *Node Structure*

A sensor node can be divided into four basic modules: transducer, processor, communications and power. The transducer module contains the physical sensing device and an analog-to-digital converter (ADC).

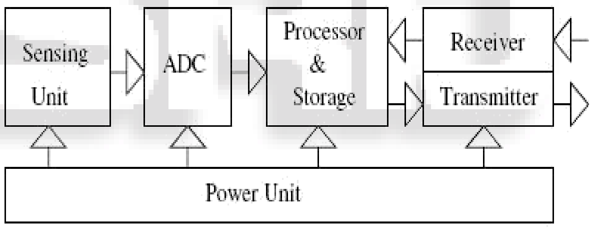

Fig. 2: Node Structure

The communication module consists of a short-range radio transceiver. The power module is used to house the battery and provides energy to the other modules. The functions of all four modules partially depend on the role of the sensor node. A sensor node can operate in one of the three roles: data collector, cluster head, or data relay. If a node is a data collector, the transducer module directly passes the sampled data to the communication module for transmission. A cluster-head node gathers the sensed data from the cluster members and performs data processing to aggregate multiple signals into one signal. If a node works as a relay, it receives the data from nearby nodes and transmits the data to other nodes or the base station.

F. *Energy Constraints*

The design of each system component can be optimized to minimize energy consumption. Energy consumption occurs in three aspects: sensing, communication, and data processing. Algorithmic modifications can often result in significant energy savings. Usually the communication of data consumes much more energy than sensing and data processing.

Energy is the scarcest resource of WSN nodes, and it determines the lifetime of WSNs. WSNs is meant to be deployed in large numbers in various environments, including remote and-hostile regions, with ad-hoc communications as key.
Therefore the algorithms and protocols are designed with the following features

- Lifetime maximization
- Robustness and fault tolerant
- Self-configuration

G. Radio Mode

The radio of a sensor node can operate in four different modes are Transmit, Receive, Idle, and Sleep. An important measurement demonstrates that idle listening dissipates very high energy, almost equal to 50-100% of the energy consumed in the Receive mode. Therefore, the radio might be scheduled to turn off completely instead of changing to the idle mode when it is not transmitting or receiving any signals. The major sources of energy waste are idle listening, collision, overhearing, and control packet overhead.

H. Access Control

Medium Access Control (shortly MAC) is used to avoid collisions by keeping two or more interfering nodes from accessing the medium at the same moment, which is essential for the successful operation of shared-medium networks. The unique characteristics of WSNs require an energy-efficient MAC that is quite different from traditional ones developed for wireless voice and data communication networks.

I. Energy Efficiency

Sensors have limited energy supply and are usually deployed in a hostile environment. Recharging is almost impossible during the operation. Therefore, long-term applications require energy-efficient solutions.

J. Scalability

Large-scale WSNs usually consist of tens of thousands of sensor nodes at least two orders of magnitude more sensors per router than conventional wireless networks. Highly localized and distributed solutions are required.

III. DYNAMIC AND AUTONOMOUS NETWORK OPERATION

Sensors are often deployed and arranged in environments that are inaccessible to humans (e.g., dropped from an airplane into remote mountainous regions). The topology of a WSN changes frequently due to failures of the sensor nodes. Therefore, protocols and algorithms with self-organizing ability are preferred.
The major performance evaluation metrics of MAC protocols are

- Power conservation.
- Average end-to-end delay.
- Throughput.
- Control overhead.

It is rather critical to operate a WSN at extremely low power levels. Although many solutions are available for conventional wireless networks, they are becoming obsolete and do not cater to present day requirements. Cellular networks, mobile ad-hoc network (MANET), and short-range wireless local area networks, however are unsuitable for achieving the unique characteristics of a large-scale WSN.

A. MAC Layer and Architecture

IEEE 802.11 MAC layer protocol is the main area of study. Since IEEE 802.11 Distributed Foundation Wireless Media Access Control (DFWMAC) is the standard for wireless ad hoc and infrastructure LANs, and it is widely used in almost all of the test beds and simulations for wireless ad-hoc networks research, an important and nature question is whether the IEEE 802.11 MAC protocol works well in multi-hop ad hoc networks.

The main job of the MAC protocol is to regulate the usage of the medium, and this is done through a channel access mechanism. A channel access mechanism is a way to divide the main resource between nodes, the radio channel, by regulating the use of it. It tells each node when it can transmit and when it is expected to receive data.

The channel access mechanism is the core of the MAC protocol. In this section, we describe TDMA, CSMA and polling which are the 3 main classes of channel access mechanisms for radio. The MAC functional description is presented in this clause. The architecture of the MAC sub-layer, including the distributed coordination function (DCF), the point coordination function (PCF), and their coexistence in an IEEE 802.11 LAN.

IV. DISTRIBUTED COORDINATION FUNCTION (SHORTLY DCF)

The fundamental access method of the IEEE 802.11 MAC is a DCF known as carrier sense multiple accesses with collision avoidance (CSMA/CA). The DCF shall be implemented in all STA, for use within both IBSS and infrastructure network configurations. For a STA to transmit, it shall sense the medium to determine if another STA is transmitting. If the medium is not determined to be busy the transmission may proceed.

The CSMA/CA distributed algorithm mandates that a gap of a minimum specified duration exist between contiguous frame sequences. A transmitting STA shall ensure that the medium is idle for this required duration before attempting to transmit. If the medium is determined to be busy, the STA shall defer until the end of the current transmission.

A. Point coordination function (shortly PCF)

The IEEE 802.11 MAC may also incorporate an optional access method called a PCF, which is only usable on infrastructure network configurations. This access method uses a point coordinator (shortly PC), which shall operate at the access point of the BSS, to determine which STA currently has the right to transmit. The operation is essentially that of polling, with the PC performing the role of the polling master.

The operation of the PCF may require additional coordination, not specified in this standard, to permit efficient operation in cases where multiple point-coordinated BSS are operating on the same channel, in overlapping physical space. The PCF uses a virtual carrier-sense mechanism aided by an access priority mechanism.

The PCF shall distribute information within Beacon management frames to gain control of the medium by setting the network allocation vector (shortly NAV) in STA. The access priority provided by a PCF may be utilized to create a contention-free (shortly CF) access method

B. Routing Protocols in WSN

Routing protocols have been developed which support establishing and maintaining the multi hop routes in MANET. These algorithms can be classified in to two different categories on-demand (reactive) such as DSR, AODV, and TORA and table driven (proactive) such as destination Sequenced Distance Vector protocol (DSDV).

C. Ad-Hoc on-Demand Distance Vector (AODV)

AODV stands for Ad-Hoc On-Demand Distance Vector and is, as the name already says, a reactive protocol, even though it still uses characteristics of a proactive protocol. AODV takes the interesting parts of DSR and DSDV, in the sense that it uses the concept of route discovery and route maintenance of DSR and the concept of sequence numbers and sending of periodic hello messages from DSDV.

Routes in AODV discovered and established and maintained only when and as long as needed. To ensure loop freedom sequence numbers, which are created and updated by each node itself, are used. These allow also the nodes to select the most recent route to a given destination node. AODV takes advantage of route tables. In these it stores routing information as destination and next hop addresses as well as the sequence number of a destination. Next to that a node also keeps a list of the precursor nodes, which route through it, to make route maintenance easier after link breakage.

To prevent storing information and maintenance of routes that are not used anymore each route table entry has a lifetime. If during this time the route has not been used, the entry is discarded.

There are three phases

1) Route Discovery
2) Route Maintenance
3) Route Determination

D. Dynamic Source Routing (DSR)

The Dynamic Source Routing protocol (shortly DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. Dynamic Source Routing, DSR, is a reactive routing protocol that uses source routing to send packets.

DSR uses source routing, i.e. the source determines the complete sequence of hops that each packet should traverse. This requires that the sequence of hops is included in each packet's header. Since finding a route is generally a costly operation in terms of time, bandwidth and energy, this is a strong argument for using source routing. Another advantage of source routing is that it avoids the need for up-to-date routing information in the intermediate nodes through which the packets are forwarded since all necessary routing information is included in the packets.

E. Route Discovery

Route Discovery is used whenever a source node desires a route to a destination node. First, the source node looks up its route cache to determine if it already contains a route to the destination. If the source finds a valid route to the destination, it uses this route to send its data packets. If the node does not have a valid route to the destination, it initiates the route discovery process by broadcasting a route request message. The route request message contains the address of the source and the destination, and a unique identification number.

F. Route Maintenance

Route Maintenance is used to handle route breaks. When a node encounters a fatal transmission problem at its data link layer, it removes the route from its route cache and generates a route error message. If though an intermediate station loses connectivity with next hop it initiates an ROUTE_ERROR message and broadcasts to its precursor nodes and marks the entry of the destination in the route table as invalid, by setting the distance to infinity.

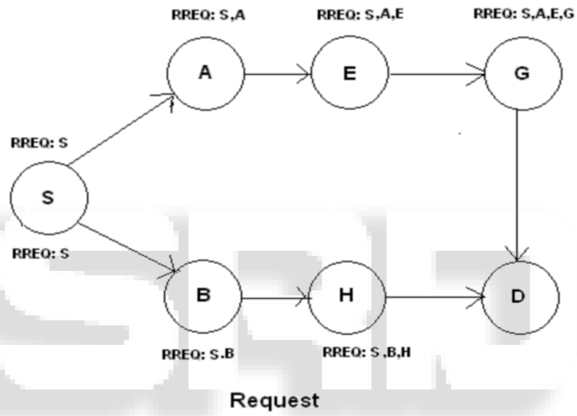

Fig. 3: Request phase in DSR

The route error message is sent to each node that has sent a packet routed over the broken link. When a node receives a route error message, it removes the hop in error from its route cache. Acknowledgment messages are used to verify the correct operation of the route links. In wireless networks acknowledgments are often provided as example. An existing standard part of the MAC protocol in use, such as IEEE 802.11.

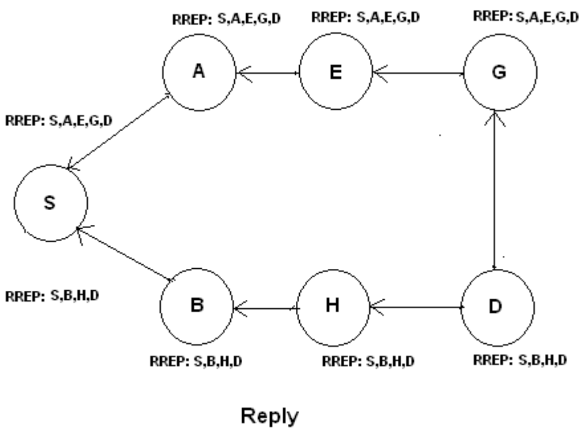

Fig. 4: Reply phase in DSR

V. Destination Sequence Distance Vector Routing (DSDV)

Destination Sequence Distance Vector (shortly DSDV) is a Proactive gateway discovery algorithm where the gateway periodically broadcasts a gateway advertisement message which is transmitted after expiration of the gateways timer. This protocol is based on classical Bellman-Ford routing algorithm designed for MANETS. Each node maintains a list of all destinations and number of hops to each destination. Each entry is marked with a sequence number.

In DSDV, a sequence number is linked to a destination node, and usually is originated by that node (the owner). The only case that a non-owner node updates a sequence number of a route is when it detects a link break on that route. An owner node always uses even-numbers as sequence numbers, and a non-owner node always uses odd-numbers.

The list which is maintained is called routing table. The routing table contains the following

1) All available destinations' IP address
2) Next hop IP address
3) Number of hops to reach the destination
4) Sequence number assigned by the destination node
5) Install time

VI. Conclusion

An energy efficient cluster based load balance routing for wireless sensor networks utilizing multipath routing to answer user queries. a novel probability model to analyze the best redundancy level in terms of path redundancy (mp) and source redundancy (ms), as well as the best intrusion detection settings in terms of the number of voters (m) and the intrusion invocation interval (TIDS) under which the lifetime of a heterogeneous wireless sensor network is maximized while satisfying the reliability, timeliness and security requirements of query processing applications in the presence of unreliable wireless communication and malicious nodes. A routing-aware optimal cluster planning and a clustering-aware optimal random relays are used for efficient load balancing.

VII. Future work

In the future, it will be necessary to have more studies on many types of algorithm that can work in many more application fields with more efficient energy use to look at infinite possibilities of sensor network used in numerous fields with numerous environment and application factorsapply the best design parameter settings at runtime in response to environment changes to prolong the system lifetime.

References

[1] Du, " Chain-based protocols for data broadcasting and gathering in sensor networks," in Proceedings of Workshop on Parallel and Distributed Scientic and Engineering Computing with Applications (in conjunction with IPDPS).
[2] Fengjun Lee and Chao "Enforcing Secure and Privacy-Preserving Information Brokering in Distributed Information Sharing" IEEE Information Forensics And Security, 2011.
[3] Haussecker "Scalable Information-Driven Sensor Querying and Routing for ad hoc Heterogeneous Sensor Networks" IEEE Personal Comm. Mag., vol 10, no. 8, jan. 2002.
[4] Praveen Rentala, "Survey on Sensor Networks" Trans. Comput. Syst., vol.24, no. 2, pp. 115–139, 2006.
[5] Huseyin Ozgur Tan, "Power Efficient Data Gathering and Aggregation in Wireless Sensor Networks", ACM SIGMOD Record, Vol. 32, No. 4, Pages 66-71, December, 2003.