isrjournals

International Journal of Advanced Research in Electronics, Communication & Instrumentation Engineering and Development

Volume: 3 Issue: 2 Dec,2016,ISSN_NO: 2347 -7210

LOCALIZATION BASED GEOCAST FOR SECURITY IN WIRELESS SENSOR NETWORK

G.Veerapandu Assistant Professor, Dept. of ECE,

Aditya Engineering College, Surampalem, Andhra Pradesh, India

ABSTRACT--*Wireless sensor network is widely used in many different scenarios. The localization information is crucial for the operation of WSN. Localization based geocast minimizes the number of radio transmissions by enhancing network lifetime and avoids traffic which in turn saves energy. Geocast sends packets to all sensor nodes within a specified geographical region in order to gather data from sensor nodes in that region. The new system proposes a location based multicast protocols for connecting geocast nodes using an energy efficient broadcasting technique without making any restrictions on the shape of the geocast region. It reduces the energy consumption during the phase of sending commands to the sensor nodes in a geocast region. Then we modify the protocol to include security mechanisms using localization to protect the data being transferred over, not only from outside attackers but also compromised inside attackers.*

Keywords: Wireless sensor networks, Geocast, Forwarding node selection.

1. INTRODUCTION

A computer network, or simply a network, is a collection of computers and other hardware components interconnected by communication channels that allow sharing of resources and information. Where at least one process in one device is able to send/receive data to/from at least one process residing in a remote device, then the two devices are said to be in a network. Simply, more than one computer interconnected through a communication medium for information interchange is called a computer network. Networks may be classified according to a wide variety of characteristics, such as the medium used to transport the data communications, protocol used, scale, topology, and organizational scope.

In a geocasting problem, a message is sent from one node to all the nodes located in a designated region. For example, a monitoring center needs to contact all active sensors within a monitored area to either gather data from them periodically or provide its location to sensors covering a certain area for event reporting. However, when a particular area containing only a small subset of active sensors needs to be monitored, the problem reduces to geocasting. Most existing geocasting solutions are shown not to guarantee delivery.

The system describes three approaches to guarantee delivery. Two of them are face traversal schemes, based on depth-first search of the face tree and traversal of all faces that intersect the border of the geocasting region, respectively. In the entrance zone multicasting-based approach, the monitoring center divides the entrance ring of a geocast region into zones of diameter equal to the transmission radius. The problem is decomposed into multicasting toward the center of each zone, and flooding from these nodes. Improvements to all methods can be made by applying neighbor or area dominating sets and coverage, and converting nodes that are not selected to sleep mode. All solutions that guarantee delivery are reported here for the first time. Network security is necessary to protect vital information.

To achieve a secure communication in Wireless Sensor Networks the following must be achieved: Data Confidentiality, Data Authentication, Data Integrity and Data Freshness.

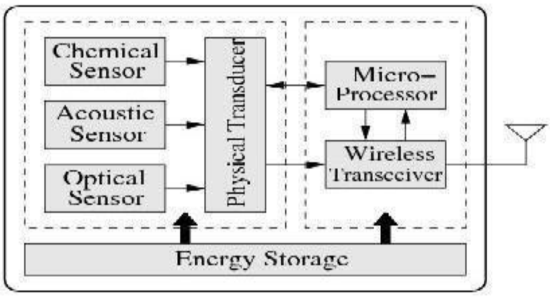

Figure 1. Wireless Sensor Network

2. GEOCASTING

Geographical routing has been applied to geocast and becomes a promising routing method for wireless sensor networks due to its simplicity. Geocast protocols can be mainly categorized based on flooding the network or on forwarding a geocast packet on a particular routing path. Here, we have presented two different location-based multicast schemes to decrease delivery overhead of geocasting packets.

A geocast packet will be lost if no enough nodes in the forwarding zone (FZ) can forward the packet to the geocast region. Figure 2 shows an example of packet loss caused by no enough nodes in the forwarding zone (FZ). In Figure 2, node A, B, and C cannot receive the geocast packets from source node S due to that no enough nodes can forward packet to them.

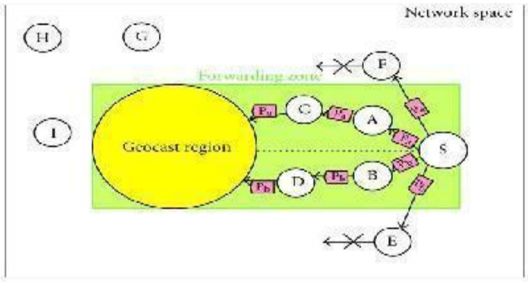

Figure 2. An example of packet loss caused by no enough nodes in the forwarding zone(FZ)

Node A cannot receive packets from source node S due to channel losses induced by the long-distance transmission. Although node D and E can receive packets from source node S, however, node D and E drop the received packets and will not forward the packets to other nodes, for example, B and C, because of node D and E are not belonging to the forwarding zone. The flooding mechanism can increase the possibility that packets can be relayed to the destined geocast region. However, it will increase the transmission overhead and network-wide data load as a tradeoff between transmission efficiency and packet reachability.

3. SYSTEM ANALYSIS

Geocast allows a sensor node to send messages to all nodes in a given geographical area without the sender node having any knowledge about which nodes are present in that area. Developing a robust geocast protocol for practical sensor networks poses several challenges. Geocast messages should be reliably delivered to the destination area in the presence of unreliable wireless links, a typical characteristic of practical sensor network deployments. The protocol should minimize the number of radio transmissions and avoid control traffic to save energy, which is a scarce resource in sensor networks. The protocol should be robust against a wide range of network densities. This paper presents the design, implementation, and evaluation of SGcast — a reliable, robust, and energy-efficient geocast protocol that achieves these goals.

3.1 Performance Evaluation

WSN is basically influenced by several factors which includes the following:

Requirement of base stations

WSNs are used to collect data from the environment. They consist of large number of sensor nodes and one or more Base Stations. The nodes in the network are connected via Wireless communication channels. Each node has capability to sense data, process the data and send it to rest of the nodes or to Base Station. These networks are limited by the node battery lifetime. The advantages are it avoids lot of wiring, can accommodate new devices at any time, flexible to go through physical partitions and it can be accessed through a centralized monitor. The disadvantages are it is very easy for hackers to hack it as we can't control propagation of waves, comparatively low speed of communications, gets distracted by various elements like Blue-tooth but it still costly at large. The base stations required are data storage for the collection of sensor patches, WAN connectivity will be wireless & base-remote link connection to the internet.

Reducing the number of transmissions

Although the use of forwarding zone can limit the number of redundant broadcasts, it just transforms the FNS problem to a problem of defining the forwarding zone the size of the zone should be large enough to allow sufficient nodes to forward the packet to achieve a high hit%, and small enough to reduce the number of radio transmissions.

Multiple values for NumNegHops

The implicit forwarding zone defined by using NumNegHops is dynamic because the value of NumNegHops is a function of current network density and link qualities. Hence different multiple values are supplied for NumNegHops which gives the current network conditions by using the propagation path already traversed by the geocast packet.

4. KEY INSIGHTS

4.1 Avoid explicit forwarding zones

Using small number of radio transmissions and achieving a high hit% are often conflicting goals because of the forwarding node selection (FNS) problem. A geocast protocol should increase the number of forwarding nodes to combat inherent unreliability of wireless links in sensor networks to achieve a high hit%. However, this also increases the total number of radio transmissions, and thus the energy consumption, in the network. On the other hand, decreasing the number of forwarding nodes reduces energy consumption, but also degrades hit%.

4.2 Dynamic heuristics

In existing protocols, a node uses static heuristics to decide whether it should forward the geocast packet. A node forwards the packet if it is in the forwarding zone. In SGcast different nodes use different heuristics depending on the amount of progress the packet has made towards the destination area. NumNegHops is a very good and natural metric that quantifies this. In SGcast, the severity of heuristics used by a node to make a packet forwarding decision is proportional to NumNegHops

4.3 Distance based backoff

In SGcast, the nodes are very closer to the destination area, and one potential issue with protocols that greedily choose nodes closer to the destination area to forward the geocast packet is the local maximum problem where geocast packet reaches a node that does not have any neighbor closer to the destination area than itself. This can prevent the packet from reaching the destination area in schemes that selects only one neighbor to forward the packet.

Forward packet flow

When SGcast receives a geocast packet to forward from the wireless medium via the underlying MAC/PHY layer, instead of copying the contents of the packet to the forward buffer, it returns a new buffer (pointer) from the forward buffer to the MAC/PHY layer and keeps the received buffer. Quickly returning the buffer to the MAC/PHY layer prevents the content of the received packet from being corrupted due to the node receiving multiple packets in a quick succession.

A packet with smallest backoff interval is placed at the head of the queue, the next spot is occupied by the packet with second smallest backoff period, and so on. The size of the priority queue is the sum of the sizes of forward and application buffers. When the packet reaches the head of the queue and backoff period expires, the packet is dequeued and heuristic check is performed again. If the check is passed, the packet is given to the MAC/PHY layer for broadcasting. Otherwise, the packet is dropped. In either case, the forwarding buffer used by the packet is freed. Note that SGcast performs the heuristic check twice. The only purpose of the first check is to save memory. A packet that fails the heuristic check before being enqueued in the priority queue fails the latter check anyway. By dropping the packet early, memory usage can be reduced.

Self-generated packet flow

When SGcast receives a request from the application layer to send a geocast packet and if the application buffer is full, it informs the application layer that the request is denied. Application layer can implement its own retransmission policy. If the application buffer is available, the packet is enqueued in the priority queue by selecting a backoff interval such that the packet is placed at the head of the queue4. The self generated geocast packet does not undergo any heuristic check because it is the first node that will transmit the geocast packet for this gid and thus the heuristic is always true.

4.5 Delivery Guarantee

It should be noted that geographic-routing-based approaches that use unicast communications for geocast can use hop-by-hop acknowledgments to provide better delivery guarantee than broadcast based approaches like HallGeocast and SGcast. Providing explicit hop-by-hop acknowledgments is difficult in broadcast based approaches because of the broadcast nature of communications. If so, the transmitter considers this as an implicit acknowledgment. Otherwise, it retransmits the packet for some threshold number of times. In this way, SGcast and HallGeocast can also provide hop-by-hop delivery guarantee.

5. CONCLUSION

In this paper we presented the design, and an extensive evaluation of SGcast a geocast protocol for WSNs. SGcast introduces several new concepts like negative hops, dynamic forwarding rules based on the path taken by geocast packets, intelligent backoff mechanism, etc. to achieve high energy efficiency without requiring local or global knowledge about the network conditions, and still maintains excellent hit%. SGcast is robust against a wide range of network conditions, mainly node densities and link disparities. We have also integrated SGcast with a localization algorithm. As future work, we plan to study the effect of localization error on the performance of the geocast protocol. Also we intend to evaluate SGcast in general MANET usage scenarios.

REFERENCES

[1] Secure and Energy-efficient Geocast Protocol for Wireless Sensor Networks based on a Hierarchical Clustered Structure, International Journal of Network Security, Vol.15, No.3, PP.151-160,May 2015, Sébastien Faye and Jean Frédéric Myoupo.

[2] R. Hall, ―An Improved Geocast for Mobile Ad Hoc Networks,‖ IEEE Transactions on Mobile Computing, pp. 254–266, 2010.

[3] An Energy-Efficient Clique-Based Geocast Algorithm for Dense Sensor Networks, Communications and Network, 2010, 2, 125-133, Alain Bertrand Bomgni, Jean Frédéric Myoupo.

BIOGRAPHY

G.Veerapandu received the B.Tech in Electronics and Communication engineering and M.Tech in Instrumentation and control systems from Jawaharlal Nehru Technical University Kakinada, India. He is currently working towards the PhD degree at the department of Electronics and Communication Engineering, Nagarjuna University, Guntur, A.P., India. His research interests in and optimization in wireless networks, and performance evaluation of protocols and algorithms.