Research About Wireless Sensor Networks

邱南藩(5070519090),才正国(5070309150),叶凝(5070309165),李逸超(5070309645)

June 30, 2010

Chapter 1

Some Routing Protocols in Sensor Networks

Abstract

Wireless Sensor Networks(WSN) is recently quickly developed and much great advancement have come about in the recent years.WSN can be used in many various application areass,for example,in nature preserves,monitoring and gathering events in hazardous environments,surveillance of buildings,and surveillance of enemy activities in a battlefield environment.For different application areas,there are different technical issues that researchers should take care of.In this paper,we first introduce the important features of WSN.Then we analyze some recent great work on WSN,this included some important protocols,some routing methods and some methods to improve the performance of WSN.After reading this paper,you would have a deep understanding of WSN and know what important features should be taken of in evaluating new research for WSN.

1.1 Introduction

Wireless sensor network is composed of tens to thousands of sensor nodes.Each sensor node consists of the five basic components:sensor unit,analog digital convector,central processing unit,power unit,and communication unit.And the most important features and requirements of a sensor network is as followed:varying network size,low cost,long network lifetime,fault tolerance,reliability,security,self-organization,query and re-tasking,cooperation among sensor nodes,application awareness,Data centric.

The routing protocols for sensor can be classified into three categories,proactive,reactive,and hybrid routing protocols.In proactive routing ,all routes are computed before.So the storage space for routing tables should be very large.While in reactive protocols,routes are computed on demand.Hybird protocols combine proactive and reactive together.

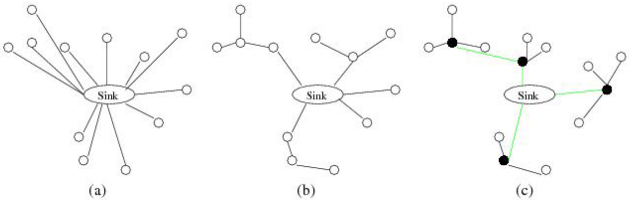


Figure 1.1. (a)direct protocol (b)flat protocol (c)cluster protocol[1]

And according to node's participating style,routing protocols can be classified into three categories,direct communication protocols,flat routing protocols,and clustering routing protocols.In direct protocol,sensor node sends its data directly to the sink.However,the larger the sensor network is,the shorter the lifetime.Under a flat routing protocol,all nodes in the network are treated equally.Different from direct protocol,when a node needs to send data,it may find a route consisting of several hops to the sink.Under a clustering routing protocol,many local sensor nodes form a cluster and select a cluster head.Members only communicate with the selected head,while the head is responsible for forwarding its members' data to the sink.Notice that this can happen directly or via other cluster heads.

1.2 Sensor Protocols for Information via Negotiation(SPIN)[1]

SPIN efficiently disseminate information among sensor nodes in an energy-constrained sensor network.Every node uses metadata to name their data and uses negotiations to eliminate the redundant data transmission.The sensor nodes can distribute data efficiently with limited energy as communication decisions are made based on application-specific knowledge of the data and knowledge of the resources that are available to it.Conventional data dissemination have three problems when they are deployed in sensor networks which is implosion,overlap,and resource blindness.SPIN solves these problems by using data negotiation and resource-adaptive algorithms.Instead of sending actual data,nodes send an ADV message which contains the metadata to the destination.If it has not received the data before,a REQ message will send back to the node,then the node will send actual data.Otherwise nothing needs to be none.This assures that there is no redundant data sent.In addition,SPIN checks the current energy level of the nodes and adapts the protocol it is running based on how much energy remains.However,SPIN has the following disadvantages.Firstly,it is not scalable.Secondly,the nodes around a sink could deplete their battery quickly if the sink is interested in too many events.Thirdly,for a given localized event,the data may be sent throughout the network.

1.3 Routing Protocols with Random Walks[1]

This algorithm achieves true multi-path routing as well as some kind of load balancing in a statistical sense.The steps for finding a route from a source to its destination.Firstly,the knowledge should be obtained first to find the requested route.The Bellman-Ford algorithm is applied to compute distances between nodes,based on the information of the source and destination unique identifiers.Secondly,each intermediate node selects one of its neighbors which are closer to the destination according to a computed probability.The advantages of this protocol are very little state information needs to be kept.It can distribute routing load or communication load at various times.Different routes are chosen at different time.The main drawback is the topology of the network may not be practical.

1.4 Rumor Routing[2]

Rumor routing is a variation of directed diffusion and is mainly intended for applications where geographic routing is not feasible.Usually directed diffusion uses flooding to inject the entire network.However,in some cases there is only a little amount of data requested from the nodes and thus the use of flooding is unnecessary.In order to flood events through the network, the rumor routing algorithm employs long-lived packets, called agents.When a node detects an event, it adds such event to its local table, called events table, and generates an agent. Agents travel the network in order to propagate information about local events to distant nodes. When a node generates a query for an event, the nodes that know the route, may respond to the query by inspecting its event table. Hence, there is no need to flood the whole network, which reduces the communication cost. On the other hand, rumor routing maintains only one path between source and destination as opposed to directed diffusion where data can be routed through multiple paths at low rates.Rumor routing performs well only when the number of events is small.The example of rumor routing protocols are MCFA,GBR,IDSQ and so on.

1.5 Cluster-Based Routing[2]

Cluster-Based routing or hierarchical routing are well-known techniques with special advantages in scalability and efficient environment.In a hierarchical architecture, higher energy nodes can be used to process and send the information while low energy nodes can be used to perform the sensing in the proximity of the target. This means that creation of clusters and assigning special tasks to cluster heads can greatly contribute to overall system scalability, lifetime, and energy efficiency.Hierarchical routing is mainly two-layer routing where one layer is used to select clusterheads and the other layer is used for routing.However,hierarchical routing is always not optimal routing and energy dissipations cannot be controlled.The famous example of cluster-based routing are LEACH,TEEN,SOP,HPAR,TTDD and so on.

1.6 Geographic Routing[3]

In this kind of routing,sensor nodes are addressed by means of their locations.The distance between neighboring nodes can be estimated on the basis of incoming signal strengths.To save energy, some location based schemes demand that nodes should go to sleep if there is no activity. More energy savings can be obtained by having as many sleeping nodes in the network as possible.The advantages of geographic routing is low-complexity,robustness and stability.However,traditional shortest path schemes(such as DSDV or AODV) and greedy geographic schemes can cause heavy throughput losses in the presence of network non-uniformities or unbalanced traffic demands.Then certain randomized strategies to route around holes were suggested but still fail in networks with typical hole configurations or provide low throughput.Then a randomized forwarding strategy by Piyush Gupta[3] based on geograhpic routing achieves near-optimal throughout over random planar networks with an arbitrary number of routing holes.

The algorithm is as followed a node on receiving a packet with the data falg checks if the final-dest id is identical to its own.If yes,it accepts the packet.Else it checks if it is on the boundary of a hole.If the node is not no the boundary of a hole.It first checks if its node location matches the next-dest.If that does not match its own location.It forwards the packet greedily towards next-dest.If it is the next-dest.Then check the stage.If stage= 0,next-dest is always FINAL-dest. The node would have already accepted the packet.if stage $= 1$ update stage= 2 and and sets next-dest = sec-dest and clears sec-dest to null, and forwards the packet to neighbor closest to the new next-dest.If stage= 2 update stage= 3 and and sets next-dest = B and forwards packet greedily towards B. If stage= 3 update stage= 4 and sets next-dest = $BB^{'}$ and greedily forwards towards next-dest. if stage= 4,update stage= 0 it sets next-dest = final-dest and greedily forwards towards next-dest.

1.7 Network Coding Based Data Collecting Routing Protocol[4]

The research on network coding has received tremendous amount of attention in recent years.The advantages of network coding are,first,network coding achieves the network multicast capacity.Second,network coding is found to be effective and helpful in lossy wireless networks.In addition,network coding is also able to utilize the wireless broadcast advantage while significantly simplifying protocol design.Finally,network coding can compress spatially correlated sensing data in a distributed fashion. In traditional routing,we usually use control messages for individual packets.However,network coding offers reliable communication and it changes the fundamental connection between end-to-end observation and link loss probabilities from product to minimum, leading to low false positives in inference algorithms.So this protocol takes advantages of network coding and as a result improve the performance in Passive loss inference problem.

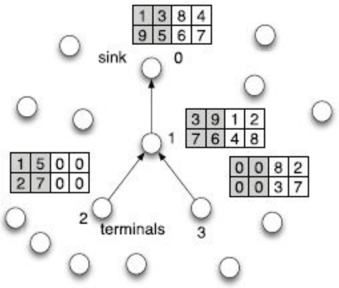


Figure 1.2. system model[4]

Network Coding Based Data Collecting Routing Protocol first rely on MintRoute[5] protocol to select the path from a terminal node to the sink.MintRoute constructs a reverse multicast rooted at the sink with all terminal nodes as the leaf nodes.Data are transmitted through the paths on the tree from terminal nodes to the sink.The terminal nodes,node 2 and 3,continuously obtain sensed data from the environment and transmit them through node 1 to the sink, node 0. All wireless links are lossy due to the inherent instability of wireless ratio.The relay node 1 performs network coding.It first checks whether the received coded packets is linearly independent with its buffered coded packets.If so,it inserts received coded packet into its buffer,otherwise,this packet is discarded.The sink decode all the source packets.Decoding is equivalent to solving a linear system composed of all coded packets received so far.The decoding matrix represents the coefficient matrix of such a linear system.

1.8 Energy Aware Routing[6]

Energy problem is a very crucial problem since sensor nodes are typically battery powered and the lifetime of the battery imposes a limitation on the operation hours of the sensor network.From the physical layer up to the network layer and application layer,researchers are investigating energy conservation at every layer.The objective of energy aware protocols is either minimizing the energy consumption or maximizing the network lifetime.Woo proposed five energy aware metrics to achieve this target.However,it is difficult to implement in a local algorithm when even the global version of the same problem is NP-complete.Chang proposed a class of flow augmentation algorithms and a flow redirection algorithm which balance the energy consumption rates among the nodes in proportion to the energy reserves.The limitation of this approach is that it requires the prior knowledge of the information generation rates at the origin nodes.A new method is the availability of the so-called energy scavengers which are devices able to harvest small amount of energy from ambient sources such as light,heat or vibration.Environmental energy is distinct from battery status in two ways.First it is a continued supply which if appropriately used can allow the system to last forever.Second, there is an uncertainty associated with its availability and measuremen.

1.9 Conclusions

Routing in sensor networks is a new area of research, with a limited, but rapidly growing set of research results.In the first project paper,we introduce some basic conception of wireless sensor network.And introduce many protocols in wsn,the latest protocols improve the former protocols very well and many great methods are proposed.For each routing protocol,no matter cluster based routing or geographic routing have their own advantages and disadvantages.Then we will introduce the opportunistic routing in detail and security problem in the wireless sensor network,giving a brief introduction about the common attacks and the related measurement.

1.10 References

[1]Q. Jiang and D. Manivannan. Routing Protocols for Sensor Networks. In Proc. IEEE (CCNC), 2004.
[2] J. N. Al-Karaki and A. E. Kamal. Routing techniques in wireless sensor net- works: a survey. IEEE Trans. on Wireless Communications $11(6), 6 - 28(2004)$.
[3] S. Subramanian, S. Shakkottai, and P. Gupta. Optimal geographic routing for wireless networks with near-arbitrary holes and traffic.In Proc. IEEE Infocom , April 2008.
[4] Y. Lin, B. Liang, and B. Li, Passive Loss Inference in Wireless Sensor Networks Based on Network Coding, in Proc. of IEEE INFOCOM 2009, Rio de Janeiro, Brazil, April 2009.
[5] A. Woo, T. Tong, and D. Culler, Taming the Underlying Challenges of Reliable Multihop Routing in Sensor Networks, in Proc. of ACM Sensys, 2003. [6]K. Zeng, K. Ren and W. Lou, Energy Aware Efficient Geographic Routing in Lossy Wireless Sensor Networks with Environmental Energy Supply, The Third International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks (QShine 2006), Waterloo, Ontario, Canada, August 7-9, 2006.

Chapter 2

Opportunistic Routing

Abstract

Opportunistic Routing is a recent technique that gets further throughput improvement,even in lossy wireless links.Traditional routing chooses the nexthop before transmitting a packet; but, when link quality is poor, the probability the chosen next hop receives the packet is low.In contrast,OR involves multiple forwarding candidates to relay packets by taking advantage of the broadcast nature and spacial diversity of the wireless medium.It is already been shown that Opportunistic Routing reaches a higher throughput than traditional routing in multihop networks.For retransmission is unlikely to occur in OR so OR is also potential in power consumption.It is already showed that network coding can bring a lot of benefits in wireless communication.We will introduce the MORE protocol which combine network coding with opportunistic routing.And in this chapter research about the end-to-end throughput of opportunistic routing in multihop multiradio and multichannel networks will be discussed.At last,as so many wireless routing protocols are proposed and will be proposed.How to evaluate these protocols is another problem will be discussed.

2.1 ExOR Opportunistic Multi-Hop Routing[1]

ExOR is an integrated routing that realizes some of the gains of cooperative diversity.ExOR broadcasts each packet,choosing a receiver to forward only after learning the set of nodes which actually received the packet.Only a single ExOR node forwards each packet,so that ExOR works with existing radios.The basic idea of ExOR is that the source broadcasts the packet.Some sub-set of the nodes receive the packet.The node in the sub-set that is closest to the destination broadcasts the packet.This continues until the destination has received the packet.One reason that ExOR provide more throughput is that each transmission may have more independent chances of being received and forwarded.Another reason is that it takes advantage of transmissions that reach unexpectedly far,or fall unexpectedly short.The forwarder list is specified based on the expected cost of delivering a packet form each node in the list to the destination.Estimated transmission count(ETX) value is used estimate the cost.ExOR uses knowledge of the complete set of inter-node loss rates to calculate these ETX values.A link's ETX value is the inverse of the link's delivery probability in the forward direction.For example,the ETX in figure is calculated as follow,the lowest ETX path is choosed.$ETX(A) = \frac{1}{0.7} + \frac{1}{0.7} = 2.86$,$ETX(B) = \frac{1}{0.9} + \frac{1}{0.85} = 2.29$,$ETX(C) = \frac{1}{0.85} = 1.17$, $ETX(D) = \frac{1}{0.7} = 1.43$.

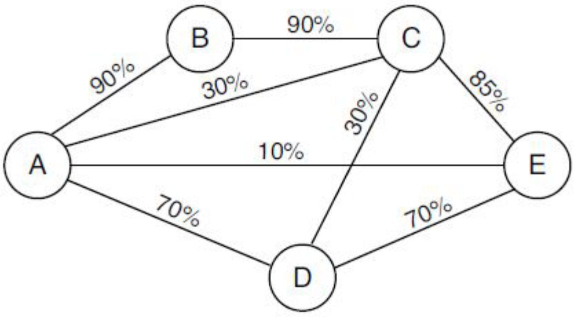


Figure 2.1. Example five node network with link delivery[1]

Compared with former protocols,ExOR requires less channel stability and takes advantage of intermediate nodes to relay packets.Former opportunistic forwarding protocols such as Geographic Random Forwarding assume that channel measurements accurately predict whether packets are likely to be delivered.In contrast,ExOR determines the forwarding node based on reception of data packets rather than preceding control packets.

2.2 MAC-independent Opportunistic Routing and Encoding[2]

Opportunistic routing allows any node that overhears the transmission and is closer to the destination to participate in forwarding the packet.Certainly it brings a lot of benefits such as low retransmission probability and high throughput.However,it also introduces a difficult challenge.Multiple nodes may hear a packet broadcast and unnecessarily forward the same packet.ExOR deals with this issue by imposing a strict scheduler on router's access to the medium and tying the MAC to the routing,and only one forwarder is allowed to transmit at any given time.In addition,some of the desirable features of the current 802.11 MAC is lost.In contrast,MORE randomly mixes packets before forwarding them.So routers hear the same transmission do not forward the same packet.

2.2.1 The Unicast Case

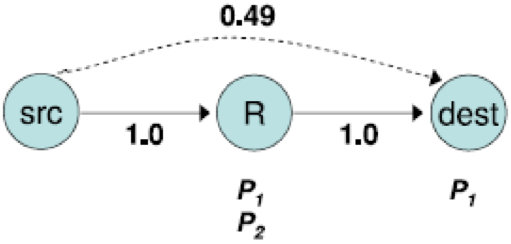


Figure 2.2. unicast example[2]

We assume that the source sends 2 packets p1 and p2.The nexthop R receives both and the destination happens to overhear p1.There is no need for R to send p1 again to the destination.ExOR requires node coordination.It imposes a special scheduler which goes in rounds and reserves the medium for a single forwarder at any one time.In MORE network coding is used to solve the solution instead of coordination.For example,R can send the sum p1+p2 and destination can get packet p2 by subtracting from the sum .In deed,the source broadcasts its packets,routers create random linear combinations of the packets they hear.The destination sends an ack along the reverse path once it receives the whole transfer.

2.2.2 The Multicast Case

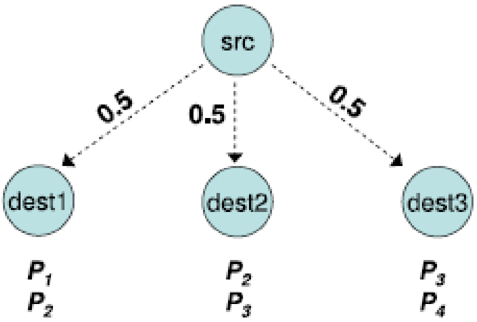


Figure 2.3. unicast example[2]

The source multicasts 4 packets to three destinations.Unluckily,each of the four packets is lost by some destination.Without network coding,the sender needs to retransmit all four packets.In contrast,with network coding,it is sufficient to transmit 2 randomly coded packets which is the linear combination of the four packets.Thus,network coding has reduced the retransmissions and improving the overall throughput.

Opportunistic routing greatly improves performance for challenged flows that usually have low throughput.When links on the best path have very good quality,there is little benefit from exploiting opportunistic receptions.However,many low-quality paths exist between the source and the destination.By using the combined capacity of all these low-quality paths,opportunistic routing manage to boost the throughput of such flows.MORE provides both unicast and multicast traffic with significantly higher throughput than both traditional routing and prior work on opportunistic routing.

2.2.3 Questions and Improvement of MORE

In the unicast example,the author strengthen the benefit of network coding and get rid of coordination.If the destination already receives p1,it can certainly decode p2 from the sum transmitted by R.However if the destination does not receive p1,it is impossible to decode p2 from the sum.And without coordination,R does not know whether the destination receives p1 or not.Maybe R continues sending the linear combination of packets it receives,destination will be able to decode all the packets sooner or later.However,with the packets increasing,such as 20 or 30 packets,R has to send a packet very large,this may cause some breakdown of the wireless network.To prevent this situation.We think that if the total packets receive by P is large than n(depends on the overhear probability) just send the linear combination of last n packets.

Network coding is greatly used in this paper,but what kind of algorithm is not mentioned.We think that soft decision networking coding may be a better choice,for the relay node may be very simple node.The basic idea of Soft Network-Coding(SoftNC)[3] is founded on the linear property of the channel code.Let U denotes the information packet and X denotes the transmitted packet and Γ denotes encode,Γ^{-1} denotes decode.The softNC can be expressed as

$$U_3 = U_1 \bigoplus U_2 = \Gamma^{-1}(X_1) \bigoplus \Gamma^{-1}(X_2)$$
$$X_3 = \Gamma(U_3) = \Gamma(\Gamma^{-1}(X_1) \bigoplus \Gamma^{-1}(X_2)) = X_1 \bigodot X_2$$

we see the relay performs networking without any channel decoding process, while the traditional NC scheme requires two channel decoding process and one channel encoding process.

2.3 Throughput Bound of Opportunistic Routing in Multi-radio Multi-channel Multi-hop Wireless Networks[4]

Two major factors that limit the throughput in multi-hop wireless networks are the unreliability of wireless transmissions and co-channel interference.So opportunistic routing is used to solve these problems.Furthermore,multi-radio and multi-channel can be used to increase the throughput bound.

2.3.1 System model

This system is a multi-hop wireless network with N nodes.Each node n_i is equipped with one or more wireless interface cards,means multi-radio.Denote the number of radios in each node n_i as t_i.Assume K orthogonal channels are available in the network without any inter-channel interference.Due to the unreliability of wireless links,there is a packet reception ratio(PRR) associated with each transmission link.Then we introduce the concept of opportunistic module for OR.It consists of a transmitter(n_i),all of its one-hop neighbors,and the wireless links associated with a PRR p_{iiq}.To avoid packet duplication,only one of the forwarding candidates becomes the actual forwarder of each packet.We use an ordered set F_i the forwarding candidate sequence to represent the forwarding priority.A forwarding candidate will forward the packet only when all the other candidates with higher priorities failed to do so.

2.3.2 Problem Formulation

The set of opportunistic modules which can be activated at the same time is named as concurrent transmission set.A CTS T_α can be represented by an indicator vector on all wireless links,written as $T_\alpha = \{\psi_{ij}^{k\alpha} | l_{ij}^k \in E\}$.

$$\psi_{ij}^{k\alpha} = \{ \begin{matrix} 1, & l_{ij}^k \text{ is usable in CTS } T_\alpha \\ 0, & \text{otherwise.} \end{matrix}$$

Denote the following indicator variable to represent the transceiver configuration status in CTS T_α:

$$\eta_i^{k\alpha} = \{ \begin{matrix} 1, & v_i^k \text{ is usable in CTS } T_\alpha \\ 0, & \text{otherwise.} \end{matrix}$$

While a usable receiver can only correspond to one transmitter.This can be represented by:

$$\eta_i^{k\alpha} = \min(1, \sum_{l_{ij}^k \in E} \psi_{ij}^{k\alpha} + \sum_{l_{ji}^k \in E} \psi_{ji}^{k\alpha}), \forall i = 1 \dots N, k = 1 \dots K$$

The number of channels being used on one node cannot exceed the number of radios installed on this node,we have:

$$\sum_{k=1}^{K} \eta_i^{k\alpha} \leq t_i, \forall i = 1 \dots N$$

The effective forwarding rate from a transmitter to its forwarding candidate sequence is the summation of the effective forwarding rate to each forwarding candidate

$$\widetilde{R}_{iF_i} = \sum_{n_{iq} \in F_i} = R_i(1 - \prod_{n_{iq} \in C_i} (1 - \phi_{iq} p_{iiq}))$$

The capacity region of the outgoing links form a transmitter n_i to its one-hop neighbors is

$$\sum_{q=1}^{L} \mu_q \phi_{iq} \leq R_i(1 - \prod_{q=1}^{L} (1 - p_{iiq} \phi_{iq}))$$

The maximum throughput problem can be converted to an optimal scheduling problem that schedules the activation of the CTS's to maximize the end-to-end throughout.

$$Max \sum_{k=1}^{K} \sum_{l_{si}^{k} \in E} \sum_{\alpha=1}^{M} \mu_{si}^{k\alpha} \tag{2.1}$$

$$\sum_{k=1}^{K} \sum_{l_{ij}^{k} \in E} \sum_{\alpha=1}^{M} \mu_{ij}^{k\alpha} = \sum_{k=1}^{K} \sum_{l_{ji}^{k} \in E} \sum_{\alpha=1}^{M} \mu_{ji}^{k\alpha}, \forall i = 1 \ldots N, i \neq s, i \neq d \tag{2.2}$$

$$\sum_{k=1}^{K} \sum_{l_{is}^{k} \in E} \sum_{\alpha=1}^{M} \mu_{is}^{k\alpha} = 0 \tag{2.3}$$

$$\sum_{k=1}^{K} \sum_{l_{di}^{k} \in E} \sum_{\alpha=1}^{M} \mu_{di}^{k\alpha} = 0 \tag{2.4}$$

$$\mu_{ij}^{k\alpha} \geq 0, \forall k = 1 \ldots K, l_{ij}^{k} \in E \tag{2.5}$$

$$\sum_{\alpha=1}^{M} \lambda_{\alpha} \leq 1 \tag{2.6}$$

$$\lambda_{\alpha} \geq 0, \forall \alpha = 1 \ldots M \tag{2.7}$$

$$\sum_{c} u_{iiq}^{k\alpha} \phi_{iq} \leq \lambda_{\alpha} R_i (1 - \prod_{c} (1 - p_{iiq}^{k} \phi_{iq})), \tag{2.8}$$

$$C = \{n_{iq} | l_{iiq}^{k} \in E, \psi_{iiq}^{k\alpha} == 1\}, \tag{2.9}$$

$$\forall v_i^k \in V, \alpha = 1 \ldots M, \forall \phi(c) \in 0, 1^{|c|} \tag{2.10}$$

The solution of the function is the upper bound of the throughput between two nodes for OR.The byproduct of the LP is the radio-channel assignment and transmission scheduling.

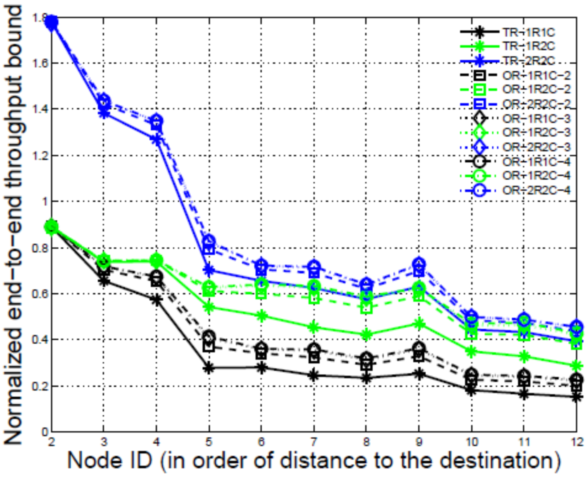


Figure 2.4. simulation result[4]

In the figure,TR represents traditional routing,OR represents opportunistic routing,xRyC-z represents x radios and y channels,with z maximal number forwarding candidates.We can see that OR can achieve better performance than TR under different radio/channel configurations. However, in particular scenarios (bottleneck links exist between the sender to relays), TR can be more preferable than OR;OR can achieve comparable or even better performance than TR by using less radio resource;for OR, the throughput gained from increasing the number of potential forwarding candidates becomes marginal.

2.4 Coordinated Anypath Routing

Coordinated Anypath Routing is an opportunistic routing designed for wireless sensor networks,in which the coordination between receivers is handled by an overhearing-based acknowledgment scheme.This protocol may be used to minimize either retransmissions or power consumption.

2.4.1 Receiver Coordination[5]

Extremely Opportunistic Routing (ExOR), designed for throughput maximization, comprises an overhearing-based coordination scheme. To choose the effective next hop, the sender includes in its packets a prioritized list of the CRS members. Next, the receivers send their acknowledgments (ACKs) in a staggered fashion, based on each node's position in the aforementioned list. As the nodes listen to each other, they include, in their own ACK, the ID of the highest-priority actual receiver they know about-possibly, their own ID. Then, all nodes believing to be the highest-priority receiver further relay the packet. The original sender of the packet considers it successfully forwarded as soon as it receives one ACK. Obviously, the emergence of multiple forwarders is not entirely eliminated, as it is not guaranteed that receivers are sufficiently able to overhear each other.

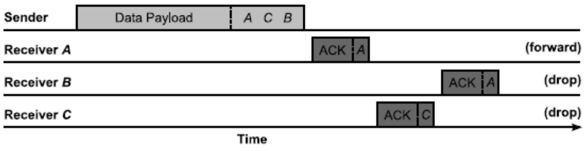


Figure 2.5. The ordered list of intended receivers[5]

Experiments show that singlepath costs will include acknowledgment costs, just as CA-Path costs do. Note that the optimal CRS determined by CA-Path is likely to be smaller than that found with anypath routing, as a larger CRS incurs a higher acknowledgment cost. Furthermore, similar to anypath routing, the cost of the shortest CA-Path route will never be higher than that of the shortest singlepath route. Although we are now considering acknowledgment costs, CA-Path still has an advantage.

For which values of p can CA-Path decrease the cost compared to singlepath. When choosing two next hops, the inequality solves to p$<$ 0.5. Thus, when p $\geq$0.5, CA-Path reduces to singlepath. Following similar reasoning, choosing three or even four next hops is interesting only when p $<$0.38 or p$<$ 0.31, respectively.

2.4.2 Minimizing Energy Consumption

CA-Path may be implemented as a purely overhearing-based, proactive routing protocol, i.e., no additional messages are required for route maintenance. Nodes must keep an up-to-date table of their neighbors' costs and include their own cost to reach the sink, together with the chosen list of intended receivers, in each data packet. Any node, overhearing this information, can update its neighborhood table accordingly. To get the process started, the sink must send out beacons, advertising its own cost of zero.

We propose the following greedy heuristic: each node evaluates its own cost w.r.t. all singleton CRSs and sorts those accordingly. Now, the node sets its CRS to be the least expensive singleton and tries to merge it with the next best one. If that decreases its cost, the node sets its CRS to be these two nodes and then tries to merge it with the third best singleton. The process is repeated until (i) the cost of the current node no longer decreases or (ii) the CRS has reached its maximum size. The experiments show that the heuristic is a good approximation of the exhaustive search for the optimal CRS.

2.5 Evaluate Routing Protocols[6]

Nowadays many routing protocols have been proposed and more will still be proposed.So research on how to evaluate these routing protocols are of great significance.The comparison between different protocols was usually in terms of Packet Delivery Ratio (PDR) and control overhead in ad hoc networks.In wireless mesh networks the main performance metric is now throughput,often times even at the cost of increased control overhead.

If you want to compare the efficiency of opportunistic routing with traditional routing.For example,ExOR and traditional routing,as ExOR is unreliable,it can only guarantees reliable end-to-end delvery of 90% of each batch,so a direct comparison of ExOR with traditional routing would be unfair.So we should do some compensation for ExOR,like making both protocols reliable.If the size of the file to be downloaded is 1MB.The evaluation of ExOR should be based on the transmission of a 1.1MB file.so as to compensate for loss.

How to compare a protocol with rate control against a protocol without.Nowadays some protocols applies sliding window-based rate control at the sources.In contrast,traditional routing has no rate control.So it is difficult to conduct a fair comparison of the two protocols.One method is that for both protocols we perform the evaluation in a saturated network,for example each source transmits at 6Mbps,same as the nominal bitrate of the network.

2.5.1 Recommendations

In the following,we make some recommendations for more consistent and meaningful evaluation methodologies.

Rate control.Rate control is fundamental for the optimal operation of any protocol,as it ensures that the traffic load does not exceed the network capacity limit.Without rate control,congestion can build up and throughput will also start decreasing when the capacity point is exceeded.By adding appropriate rate control,the goodput is expected to remain constant when the offered load is beyond the capacity.A related recommendation is that a protocol should also be evaluated with multiple flows.

Isolating the benefit from new optimization techniques.The evaluation of a new protocol that exploits a new optimization technique should try to isolate the gain from this technique, alone. The tricky part here is that in adding a new optimization technique, a new protocol often incorporates other old techniques brought down to the routing layer from the upper layers, such as end-to-end reliability and rate control.

Separating rate control form end-to-end reliability.When comparing a new reliable protocol to an unreliable one,the simplest method to add end-to-end reliability to the unreliable routing protocol is to run it under TCP.One should attempt to incorporate the relaibility/rate control features of the new protocol to the protocol,the comparison will be able to isolate the gain from the technique exploited in the new protocol.

2.6 Conclusion

In project report2,we focus on research about opportunistic routing.First we introduce MORE,which uses MAC independent instead of coordination,and we also propose some mechanism for network coding in MORE.Then we introduce the throughput bound of opportunistic routing in multi-radio multi-channel multi-hop wireless networks as the extension of throughput bound in multi-hop networks introduced in project1.And get some interesting results in this system.Then we show the potentials of opportunistic routing in energy-constrained and data gathering.At last,we do some research about how to evaluate these routing protocols and give some recommendation.

2.7 References

[1] S. Biswas and R. Morris. ExOR Opportunistic Multihop Routing for Wireless Networks. In Proc. of the ACM SIGCOMM Conf. pages 133 – 144, Philadelphia, PA, Aug. 2005. [2] S. Chachulski, M. Jennings, S. Katti, and D. Katabi. Trading structure for randomness in wireless opportunistic routing. In ACM SIGCOMM, 2007.

[3]Shengli Zhang, Yu Zhu Soung-chang Liew,"Soft Network Coding in Wireless Two-Way Relay Channels."

[4] K. Zeng, Z. Yang, and W. Lou, "Opportunistic Routing in Multi-radio Multi-channel Multi-hop Wireless Networks", IEEE Infocom Mini-Conference 2010, San Deigo, CA, March 15-19, 2010.

[5] SCHAEFER, G., INGELREST, F., AND VETTERLI, M. 2009. Potentials of opportunistic routing in energyconstrained wireless sensor networks. In Proceedings of the IEEE EuropeanWorkshop onWireless Sensor Networks and Applications (EWSN).

[6] Dimitrios Koutsonikolas, Y. Charlie Hu, and Konstantina Papagiannaki. How to evaluate exotic wireless routing protocols? In Proc. of ACM HotNets-VII, 2008

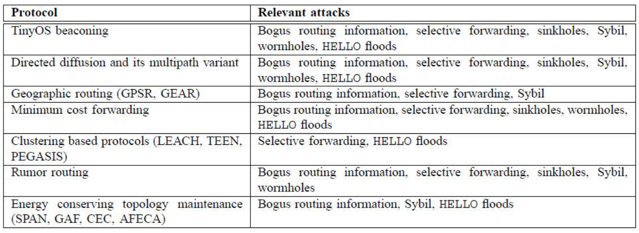
Chapter 3

Security

Abstract

In this chapter we will introduce the security problem in wireless sensor networks.Security is always a very hot and important topic in networks.Expecially for wireless sensor networks,which aims for military applications.In this chapter,we will introduce the general concepts about security in WSN,network layer attacks categories and the related countermeasures.

3.1 Security Of Wireless Sensor Network[1]



Protocol	**Relevant attacks**
TinyOS beaconing	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods
Directed diffusion and its multipath variant	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes, HELLO floods
Geographic routing (GPSR, GEAR)	Bogus routing information, selective forwarding, Sybil
Minimum cost forwarding	Bogus routing information, selective forwarding, sinkholes, wormholes, HELLO floods
Clustering based protocols (LEACH, TEEN, PEGASIS)	Selective forwarding, HELLO floods
Rumor routing	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes
Energy conserving topology maintenance (SPAN, GAF, CEC, AFECA)	Bogus routing information, Sybil, HELLO floods

Figure 3.1. summary of attacks against proposed sensor networks routing protocols[1]

The threat models: An important distinction can be made between mote-class attackers and laptop-class attackers. In the former case, the attacker has access to a few sensor nodes with similar capabilities to our own, but not much more than this. In contrast, a laptop-class attacker may have access to more powerful devices, like laptops or their equivalent. Thus, in the latter case, malicious nodes have an advantage over legitimate nodes. A second distinction can be made between outsider attacks and insider attacks. We have so far been discussing outsider attacks, where the attacker has no special access to the sensor network. One may also consider insider attacks, where an authorized participant in the sensor network has gone bad.

3.1.1 Network Layer Attacks Categories

- spoofed, altered, or replayed routing information, The most direct attack against a routing protocol is to target the routing information exchanged between nodes.

- selective forwarding, In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further.

- sinkhole attacks, In a sinkhole attack, the adversary goal is to lure nearly all the traffic from a particular area through a compromised node,creating a metaphorical sinkhole with the adversary at the center.

- Sybil attacks, In a Sybil attack, a single node presents multiple identities to other nodes in the network. The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes.

- wormholes, In the wormhole attack, an adversary tunnels messages received in one part of the network over a low-latency link and replays them in a different part.

- HELLO flood attacks, Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within normal radio range of the sender. This assumption may be false for a laptop-class attacker broadcasting routing or other information with enough power could convince every node in the network that the adversary is its neighbor.

- acknowledgement spoofing. Due to the inherent broadcast medium, an adversary can spoof link layer acknowledgements for ”overheard” packets addressed to neighboring nodes in order to convince the sender that a weak link is strong or even more that a dead/disabled node is alive.

3.1.2 Countermeasures

- outsider attacks and link layer security The majority of outsider attacks against sensor network routing protocols can be prevented by simple link layer encryption and authentication using a globally shared key. Thus the Sybil will not be relevant because no matter how many identities the adversary has, she doesn't have the right key. Anyway link layer encryption and authentication cannot deal with attacks like wormhole and HELLO flood attacks, and the mechanisms using a globally shared key are ineffective in presence of insider attacks or compromised nodes.

- the Sybil attack Identities must be verified but it's a pity that generating and verifying digital signatures is beyond the capabilities of normal sensor nodes. One solution is to have every node share a unique symmetric key with a trusted sink. Then we have protocols like Needham-Schroeder for nodes to verify each other's identity and establish a shared key. A pair of neighboring nodes can use the resulting key to implement an authenticated, encrypted link between them. This is not to say that nodes are forbidden from sending messages to sinks or aggregation points multiple hops away, but they are restricted from using any node except their verified neighbors to do so. In addition, an adversary can still use a wormhole to create an artificial link between two nodes to convince them they are neighbors, but the adversary will not be able to eavesdrop on or modify any future communications between them.

- HELLO flood attacks The simplest defense against hello flood attacks is to verify the bidirectionality of a link before taking meaningful action based on a message received over that link. However, this countermeasure is less effective when an adversary has a highly sensitive receiver as well as a powerful transmitter. Since the links between these nodes and the adversary are bidirectional, the above approach will unlikely be able to locally detect or prevent a hello flood. One possible solution is for every node to authenticate each of its neighbors with an identity verification protocol using a trusted sink, so an adversary claiming to be a neighbor of an unusually large number of the nodes will raise an alarm.

- wormhole and sinkhole attack Wormholes are hard to detect because they use a private, out-of-band channel invisible to the underlying sensor network. Sinkholes are difficult to defend against in protocols that use advertised information such as remaining energy or an estimate of end-to-end reliability to construct a routing topology because this information is hard to verify. One class of protocols resistant to these attacks is geographic routing protocols which construct a topology on demand using only localized interactions and information and without initiation from the sink. Artificial links are easily detected in geographic routing protocols because the ”neighboring” nodes will notice the distance between them is well beyond normal radio range.

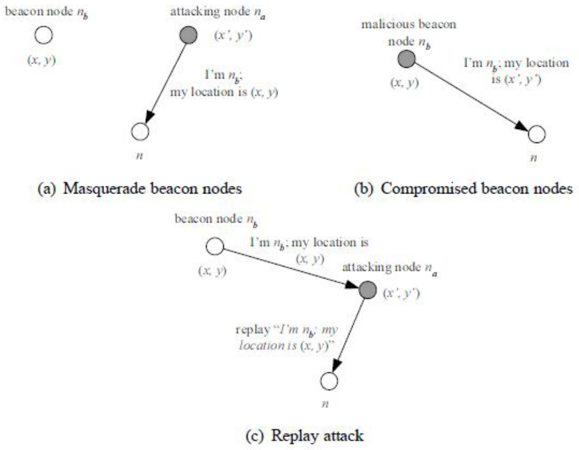
- selective forwarding A compromised node has a significant probability of including itself on a data flow to launch a selective forwarding attack if it is strategically located near the source or a sink. Multipath routing can be used to counter these types of selective forwarding attacks. The use of multiple braided paths may provide probabilistic protection against selective forwarding and use only localized information. Allowing nodes to dynamically choose a packet's next hop probabilistically from a set of possible candidates can further reduce the chances of an adversary gaining complete control of a data flow.

- authenticated broadcast and flooding Authenticated broadcast is useful for localized node interactions. Many protocols require nodes to broadcast HELLO messages to their neighbors. These messages should be authenticated and impossible to spoof. Flooding can be a robust means for information dissemination in hostile environments because it requires the set of compromised nodes to form a vertex cut on the underlying topology to prevent a message from reaching every node in the network. The downsides of flooding include high messaging and corresponding energy costs, as well as potential losses caused by collisions. But we have protocols like SPIN and gossiping algorithms to reduce messaging cost and collisions.

3.2 Attack-resistant location estimation[2]

Without protection, an attacker may easily mislead the location estimation at sensor nodes and subvert the normal operation of sensor networks. we investigate two types of attack-resistant location estimation techniques to tolerate the malicious attacks against range-based location discovery in wireless sensor networks. The first technique, named Attack-Resistant Minimum Mean Square Estimation (AMMSE), is based on the observation that malicious location references introduced by attacks are intended to mislead a sensor node about its location, and thus are usually inconsistent with the benign ones. Our second technique, a voting-based location estimation method, quantizes the deployment field into a grid of cells and has each location reference ”vote” on the cells in which the node may reside.

For AMMSE: Intuitively, a location reference introduced by a malicious attack is aimed at misleading a sensor node



(a) Masquerade beacon nodes

(b) Compromised beacon nodes

(c) Replay attack

Figure 3.2. attacks against location discovery schemes[2]

about its location. Thus, it is usually "different" from benign location references. When there are redundant location references, there must be some "inconsistency" between the malicious location references and the benign ones. An attacker may still have a location reference consistent with the benign ones after changing both the location and the distance values. However, such a location reference will not generate significantly negative impact on location determination. To take advantage of this observation, we propose to use the "inconsistency" among the location references to identify the malicious ones, and discard them before finally estimating the locations at sensor nodes.

For voting-based location estimation In this approach, we have each location reference "vote" on the locations at which the node of concern may reside. To facilitate the voting process, we quantize the target field into a grid of cells, and have each sensor node determine how likely it is in each cell based on each location reference. We then select the cells with the highest vote and use the "center" of the cells as the estimated location. To deal with the resource constraints on sensor nodes, we further develop an iterative refinement scheme to reduce the storage overhead, improve the accuracy of estimation, and make the voting scheme efficient on resource constrained sensor nodes.

Both proposed techniques can usually remove the effect of the malicious location references from the final location estimation when there are more benign location references than the malicious ones. When the majority of location references are benign, the location estimation error of the attack-resistant MMSE is bounded if we can successfully identify the largest consistent set. Hence, to defeat the attack-resistant MMSE approach, the attacker has to distribute to a victim node more malicious location references than the benign ones, and control the declared locations and the physical features like signal strength of beacon signals so that the malicious location references are considered consistent.

3.3 Conclusion

So far, we have introduced 7 kinds of attacks and 6 kinds of countermeasures dealing with different kinds of attacks. I New kinds of attacks come into being one after another, so do the measures to prevent the attacks.The basic ways to prevent attacks are,first,improve the protocol itself and leave no aws for attackers.Second,get enough understanding of the attack methods so we can get prepared well enough to beat the attacks.

3.4 References

[1] Chris Karlof , David Wagner: Secure routing in wireless sensor networks: attacks and countermeasures, Ad Hoc Networks $1(2003)293 - 315$
[2]Donggang Liu, Peng Ning, An Liu, Cliff Wang, Wenliang Kevin Du, Attack-Resistant Location Estimation in Wireless Sensor Networks, Proceedings of The Fourth International Symposium on Information Processing in Sensor Networks $(IPSN'05), pages99 - 106$, April 2005

Chapter 4

Our Own Routing Protocol

Abstract

In the former chapters,we have learned many kinds of routing protocols and get a brief understanding of many technologies about routing protocol in wireless sensor network.So we try to come up with our own protocol routing and introduce it in this chapter in detail.

4.1 Protocol Introduction

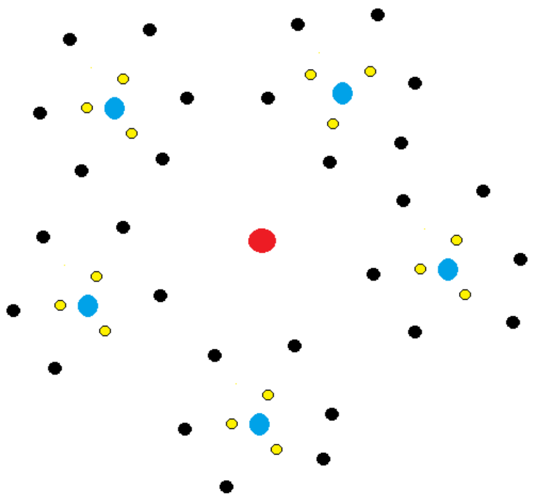


Figure 4.1. System Model

In figure 4.1 is our system model.This model is based on clustering routing.The black node is local sensor nodes.They only collect the data we need and send the data to its next hop candidates and finally to the cluster head.The yellow nodes is more than local sensor nodes,they can not only collect the local data,but also act as the opportunistic candidate and perform network coding,which we will introduce in detail later.The blue nodes are cluster head,they should be nodes with large storage ability and computation ability.For they should store the information of all the local sensor nodes and perform decoding.The red node is the sink,all the cluster head send their local data to the sink node either directly or through other cluster heads as the relay.There are four advantages of this routing architecture.First,it is scalable.Secondly,it simplifies the process of finding an available route to a destination.Thirdly,it is energy efficient,since it is easy for a cluster head to suppress duplicated sensed data collected by different cluster members.Finally,it is easier to manage the sensors and routes.

Then we will introduce how the local sensor nodes communicate with the cluster head.As we have showed in chapter2,opportunistic routing performs very well in lossy wireless links network.In addition,opportunistic routing reaches a higher throughput.So local sensor nodes select a set of opportunistic candidates as the next hop.Which is the yellow nodes and blue nodes in the graph.Certainly the cluster head has the first priority.Other candidates are yellow nodes near the cluster.If they are far away from cluster head,the probability they receive the packet is low.And how many candidates depends on the strength of wireless links.If environment is well and links are good.We choose less candidates,in other words,use less yellow nodes.In the other way,if environment situation is very tough,more yellow nodes will be used in the system model.In addition,this method can also improve protocol’s security as it chooses next hop from a set of possible candidates so that it is hard for the attackers to know which route to break.Even if some candidates break down,as long as the cluster heads work well,the system will not break down.

Network coding will also be used in our model.As we have introduced,network coding can achieve the network multicast capacity.Second,network coding is found to be effective in lossy wireless networks.In addition,network coding is also able to utilize the wireless broadcast advantage and can compress spatially correlated sensing data in a distributed fashion.In our model,if any yellow candidate node receives the packet.They do the linear combination of all the packets it receives and send it to the cluster head.When the cluster head has received enough linear combination packets.It sends a message to the local nodes to stop them from sending.Decoding is equivalent to solving a linear system.

As the way cluster head communicates with the sink,we choose the geographic routing.For in our model,the cluster head can not move around and they are aware of location information.And these cluster heads are special nodes,their wireless links are strong and the probability of packets being successfully received is high.In this situation,geographic routing is a good choice.For they already know the location information before,so it is possible to compute the best routs in advance.The advantages of geographic routing is low-complexity,robustness and stability.

Next we will consider the mobility of the system model.In our model,the local sensor black nodes and yellow candidate nodes are mobile nodes which can move around.But the cluster head and sink can not move.As we know,mobility can increase the capacity of system.In addition,sensor nodes with mobility can visit more source targets ,searching for unknown data sources.So this architecture have some advantages in improving the performance.Our strategy is that every cluster head has their own effective regions.The nodes within this region will send packet to the region cluster head.So avoid the situation that sensor node is far away from cluster head because of mobility.But we should also avoid the ping-pong effect of sensor node.For example,a sensor node is near the edge of two cluster heads region.It is possible that it will change its cluster head now and then because of mobility.So we apply the idea soft handoff into our protocol.The sensor node receive acknowledge messages from different near cluster heads.For the broadcast nature of message,this is possible,only when message from one cluster head is larger than others and the difference surpasses a gate value.The sensor node will change its belonging cluster head.So in this way the ping-pong effect is avoided.

4.2 Conclusion

In this chapter,we come up with ideas about our own protocol routing.In this routing protocol,we based on cluster structure,apply ideas about opportunistic routing ,network coding and geographic routing into our protocol.We also do some analysis in mobility problem in our protocol and sign up the soft handoff method to solve the ping-pong effect.

4.3 Group Members

Figure 4.2. Group Members

The left one is Zhengguo Cai,his main contribution is research about traditional routing protocols in sensor network. The middle one is Ning Ye,his main contribution is research about security problem in sensor network. The right one is Nanfan Qiu,he is the group leader who arrange the process of our project and combine group members' work together.His main contribution is research about many previous routing protocols and come up with our own routing protocol. The bottom one is Yichao Li,his main contribution is research about opportunistic routing protocols. At last,we are all very thankful to Doctor Wang and TA's great help.