International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.2, Issue.6, Nov-Dec. 2012 pp-4122-4127 ISSN: 2249-6645

The Minimum Cost Forwarding Using MAC Protocol for Wireless Sensor Networks

M.Chithik Raja
Department of Information Technology
Salalah College of Technology
Sultanate of OMAN

ABSTRACT:*Many routing protocols have been proposed to facilitate data transport from sensor nodes to a base station; few of these protocols have been formally verified or operationally deployed however. The Minimum Cost Forwarding (MCF) routing protocol in MAC layer, has been proposed. The application of MCF is restricted to networks possessing a single sink node and multiple source nodes. However, it offers several potential advantages for sensor nodes with limited resources. The MCF protocol is the subject of the current study with a view to its implementation in a prototype sensor network. The first phase of the work, and the subject of this paper, is the formal evaluation of the MCF protocol to increase confidence in its correctness and study its ability to handle node failure and other errors. As a result of formal verification using a model checking tool, UPPAAL, we confirm the soundness of the protocol during its initialization and operational phases and we have identified significant weaknesses in the published protocol concerning equal-cost minimum cost paths and node failure. In particular, we identify a flaw in the previously suggested periodic initialization broadcast to reestablish a minimum cost field. Here we present these results and offer improvements to overcome some deficiencies. It is expected that model checking may usefully be applied in the study of other WSN protocols.*

I. INTRODUCTION

Sensor networks have been researched and deployed for decades; their wireless extension, however, has witnessed a tremendous upsurge in recent years. This is mainly attributed to the unprecedented operating conditions of wireless sensor networks (WSNs). As of today, a major problem in deploying WSNs is their dependence on limited battery power. A main design criterion is to extend the lifetime of the network without jeopardizing reliable and efficient communications from sensor nodes to other nodes as well as data sinks. A prominent example of today's non-optimized WSN deployment experiences is that the start-up alone costs the network a third of its battery power [1][2]. Optimizing every facet of the communication protocols is therefore vital and imperative. Such stringent design requirements can be met by a plethora of approaches, e.g. using cross-layer design paradigms, collaborative protocols, etc. This has led to copious novel distributed signal processing algorithms, energy-efficient medium access control and fault-tolerant routing protocols, self-organizing and self-healing sensor network mechanisms, reliable data aggregation algorithms, etc. These solutions stipulated first commercial activities as well as standardization approaches, including WOSA [3], KNX [4], IEEE 802.15.4 [5], IETF 6LowPan [6], IETF ROLL [7], etc.

Wireless sensor networks (WSN) consist of small self contained devices with computational, sensing and wireless communication capabilities. When deployed, they allow flexible, powerful, tether-less, automated data monitoring and/or control systems to be created. A sensor network comprises a set of sensor nodes and one or more base stations. The sensors generate, process and forward data via intermediate nodes to the base stations. Anticipated applications include environmental hazard monitoring, forest fire detection, machine instrumentation, etc. SensorNetworking has received considerable attention in recent years and many routing protocols have been proposed to facilitate data transport over such networks. Our current work[4] is based on the Minimum Cost Forwarding (MCF) network routing protocol in MAC layer with the view to its implementation in a prototype sensor network. The first phase of the work, and the subject of this paper, is the formal evaluation of the MCF protocol to increase confidence in its correctness and study its ability to handle node failure and other errors in MAC Protocol. MCF is considered particularly appropriate for sensor networks possessing limited resources since it does not require the storage of routing tables at sensor nodes, it establishes optimal routing paths with few message exchanges and it is scalable and simple to implement. The MCF protocol adopts a so-called *flat* model in which nodes have equal status except for a single base station, i.e. there is no hierarchy amongst the nodes. All message traffic generated at sensor nodes is routed towards a base station by forwarding along minimum cost paths comprising one or more sensor nodes.

The minimal cost path field is established during an initialization phase after which message traffic may commence. We describe in this paper how the MCF routing protocol may be formally modeled as a set of timed automata. The models are amenable to a formal analysis to verify that they possess some well-defined properties. Our aim is to investigate if MCF can successfully establish a minimum cost field and that data generated periodically at sensor nodes is communicated to a base station. Additionally we study the problems of node failure and equal-cost paths which compromise the effectiveness of MCF. Our focus is not merely to restatethe MCF protocol but to present a formal verification of its behavior and to identify some of its operational difficulties. The remainder of this paper is organized as follows. In Section II, we describe the operation of the Minimum Cost Forwarding protocol. We present the algorithms used to establish a minimum cost field over a group of sensor nodes and to forward frames generated in sensor nodes to a base station.

II. MAC Protocols

MAC protocols developed for WSNs may be grouped into two main approaches: Scheduled-Based and Contention-Based [15]. Schedule-Based protocols regulate medium access by defining an order or Schedule for nodes to transmit, receive or be inactive. Examples of Schedule- Based protocols include: PEDAMACS, TRAMA and NATP. Power Efficient and Delay Aware Medium Access Protocol (PEDAMACS) [16] however generates overhead traffic needed for synchronizing the nodes and for topology adjustment, Traffic-Adaptive Medium Access Protocol (TRAMA) [15], whose overhead comes from exchanging neighbor and schedule information, and Neighbor Aware Probabilistic Transmission Protocol (NATP) [17], which creates overhead with neighbor information and synchronization beacons. Contention-Based protocols do not require central coordination but they use energy during periods of "Idle listening", which occurs when nodes are listening to the medium and there are no transmissions, thus wasting energy [18]. Sensor MAC (S-MAC) [18] operates in a similar way to 802.11: RTS, CTS and ACK frames are exchanged in order to send data. Additionally, nodes in S-MAC go tosleep and wake up following a schedule given by a SYNC frame. Control frames generate overhead. Timeout MAC (T-MAC) [19] improves on S-MAC energy consumption following the same basic idea: using a schedule for sleeping and waking up. However, T-MAC makes nodes sleep earlier during the schedule if there are no activation events, such as the node needing to send information or hearing activity in the channel. As in S-MAC case, RTS, CTS, ACK and SYNC frames generate overhead. Polastre et al introduced the Berkeley MAC (B-MAC) [20], protocol with no control frame overhead. B-MAC uses a long preamble in data frames and nodes verify the medium periodically, with a period equal to the preamble size. When they are not verifying the medium, nodes go to sleep. However, the preamble itself creates overhead to ensure nodes will check the medium in the proper time. One example results in transmitting 271 bytes for sending 36 bytes of data [20]. Uncertainty Driven MAC (UBMAC) [21] reduces preamble size from B-MAC by estimating clock uncertainty using Rate Adaptive Time Synchronization (RATS). RATS exchanges frames with timestamps between neighbors and computes clock uncertainty within an error boundary, allowing smaller preambles when used over B-MAC. On the other hand, there is a learning phase for the protocol which generates additional overhead besides timestamp frames. Sift [3] is a CSMA type of protocol using a non-uniform probability distribution for selecting the backoff waiting time. S-MAC, B-MAC and 802.11 use Binary Exponential Backoff with uniform probability for selecting the backoff time. Sift has a significantly smaller delay than 802.11 when several sources are sending data in the same zone of the network. The protocol uses RTS, CTS and ACK frames when the packet size is big, but there is no control frame overhead for small packets. However, there is no provision for turning off the radio, so idle listening occurs. To conserve energy many MAC protocols turn off the radio. A routing protocol using any of these MAC protocols must find new routes very frequently, since topology changes not just when nodes die, but also when they are temporarily out of the network due to MAC functionality. Protocols such as GSP do not compute routes, so they may be suitable to work these MAC protocols. However, GSP itself decides when to turn on or off the radio, and to optimize performance, those decisions must agree with the characteristics of the MAC layer. As an example consider using S-MAC or T-MAC with GSP, the Gossip Period must harmonize with the SYNC schedule and all transmissions and sleeping periods must be decided in advance, after considering the Gossip Probability. GSP and Sift do not generate conflicts in changing the radio state but both protocols most exchange state information in order to send a packet, because the radio is on and also the appropriate backoff time has elapsed. Arbitrating the interaction between MAC and Routing protocols adds complexity, additional places where errors may be introduced and the opportunity for hackers to find protocol exploits.

III. Minimum Cost Forwarding Algorithm

Minimum Cost Forwarding Algorithm (MCFA) computes the least cost from each node to the Base Station (BS). If the node is in the shortest path, the node retransmits the data; the same procedure repeats until the packet reaches the BS. Nevertheless, computing and updating the Minimum Cost generates overhead. A Gossiping protocol requires that a node receiving a packet retransmit it with a probability less than 1.0, which improves upon flooding performance because if the packet is not retransmitted, there is one less duplicate in the network. However, sensor nodes using Gossip waste energy receiving a packet if that packet is not retransmitted. The Gossip-based Sleep Protocol (GSP) improves on Gossiping because it drops a packet by not receiving it. If a acket is received it will be etransmitted, so energy spent for receiving is not wasted. GSP divides time in Gossip Periods with fixed duration [4]. At the beginning of each gossip period, every node decides with robability p, the Gossip Probability, to turn off its radio, and with probability (1-p) to turn it on, ready to receive. A node receiving one packet must retransmit it in the following gossip period. All sleeping nodes must wake up in the next gossip period. Figure 1 shows one example of GSP. A node can be in one of three possible states: On Receiving, On Transmitting and Off.

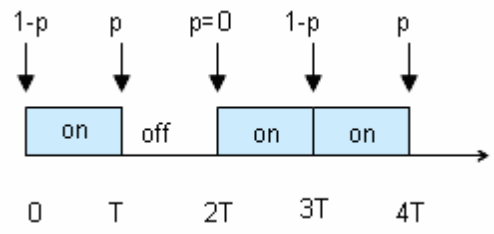

Fig. 1 One node using GSP. Each gossip period has duration T.

A. Initialization Mode

To begin establishing a minimum cost field the base station generates a single advertisement message with a cost of zero:

Begin { *Base Station, INIT protocol* }
Broadcast ADV with node cost 0;
End

A general node, i, sets its minimum cost, Li, to infinity and waits for *ADV* messages to arrive each containing a cost field, Lm. If the value of the cost field plus the link cost is less than the current minimum cost, the node updates its minimum cost and sets its timer to expire after _Ci,m. As *ADV* messages with lower costs arrive, the timer may be reset several times before it expires. When the timer finally expires, the node broadcasts its *ADV* message advertising its minimum cost. The backoff time is thus proportional to the minimum cost at a node. Thus, a node will defer its *ADV* broadcast until it has heard the message leading to the minimum cost and make a single broadcast carrying its minimum cost.

Begin { *Node i, INIT protocol* }
Li := 1;
loop
Receive an ADV message from node m;
if (Li > Lm + Ci,m**)**
Reset backoff timer to expire after _Ci,m;
else
Discard ADV message;
End loop
EVENT - backoff timer expires
Broadcast ADV with node cost Li;
End

This backoffscheme suggested by Ye et al is a meansof reducing the overall number of *ADV* broadcasts comparedto simply rebroadcasting every *ADV* that is received. Theirsimulation study showed that by selecting a value of approximately equal to the propagation and software delays,few nodes made broadcast more than once.

B.Operational Mode

Once the cost field has been established, nodes engage inthe*OPER* mode protocol. The base station simply consumes*DATA*messages forwarded by nodes:

begin{*Base Station, OPER protocol* }
loop
Read and store DATA message;
endloop
end

DATA messages contain the data collected at a sensornode, the original cost and the consumed cost, as depictedin**Figure** 2.

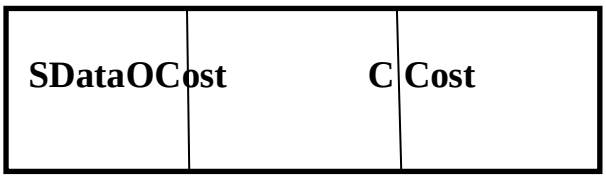

Fig. 2. DATA message fields

A general node in *OPER* mode must forward *DATA* messagesit receives after checking first that they are from transmittingnodes on a minimum path; messages containing costsgreater than the minimum cost are ignored. The consumedcost of the message is computed before it is forwarded.Periodically, a node generates its own sensor *DATA* messagesfor forwarding.

begin{*Node i, OPER protocol* }
loop
Receive a DATA message from node m;
if(Li >OCostm)
Drop DATA message;
else
CCost :=CCostm + Ci,m
if(Li = OCostm − CCost)
Broadcast DATA message (SDatam,OCostm,CCost);
else
Drop DATA message;

Endloop
EVENT - sensor data available from instrument
Broadcast DATA message with the local data,OCost = Li and CCost = 0;
End

IV. Scheduled MAC Protocols

Periodic and high-load traffic is most suitably accommodated by means of reservation-based protocols, i.e. those which build a specific schedule. Generally, in the context of WSNs, such protocols are variants of TDMA (Time Division Multiple Access) combined with FDMA (Frequency Division Multiple Access) where different time slots and frequency channels can be used by different nodes. TDMA is attractive because – once the schedule is set up – there are no collisions, no overhearing, and minimized idle listening. In addition, TDMA offers bounded latency, fairness and good throughput in loaded (but not saturated) traffic conditions. The central concern of TDMA type protocols is how to set up and maintain a specific schedule. To this end, three methods are used in the context of WSNs:

Scheduling of communication links: This fairly traditional approach sets up a unique slot dedicated to a specific sender and specific receiver, thereby minimizing idle listening and eliminating collisions and overhearing. Since transmitter and receiver know exactly when to wake up, this is the most energy efficient solution given the schedule is set up and that packets need to be transmitted; however, varying traffic conditions, imprecise clocks and network dynamics require new schedules to be set up which incurs large overheads.

Scheduling of senders: In this approach the slot is specified which is used by the sender which requires all receiving nodes to listen. It hence minimizes idle listening, eliminates collisions and reduces overheads to a certain extend (since any changes at the receiving side remain transparent to the established schedule); however, overhearing remains a problem of such an approach. A node, however, may minimize overhearing further through header filtering, i.e. when the packet is destined to another node, the receiver goes back sleeping during that slot.

Scheduling of receivers: Here, the receiving slots are specified. Overhearing is eliminated, idle listening minimized and overheads are reduced (since network dynamics at the transmitting side are transparent to the schedule). However, collisions between various transmissions can potentially occur if more than one transmitter wishes to reach a specific receiver; suitable contention resolution methods are hence needed. The first two variants of TDMA are suited to periodic, delay sensitive and fairly high-load traffic, the third to periodic and medium-load traffic. Whilst many variants of above protocols exist, such as the beacon-enabled guaranteed time slot transmission during the collision free period of the IEEE 802.15.4 MAC to be exposed in Section 6, we shall discuss the recently emerged Time Synchronized Mesh Protocol (TSMP) [22] to exemplify its functioning. TSMP is TDMA-based and hence requires network-wide synchronization. Access is controlled by means of a tunable amount of timeslots which form a frame. The protocol is designed such that a node can participate in multiple frames at once allowing it to have multiple refresh rates for different tasks. TSMP employs in addition FDMA and frequency hopping, i.e. different links use differing frequency slots and the same link hops during its life time across different frequency slots. This yields high robustness against interference and other channel impairments. A traditional approach to facilitate synchronization is beaconing, where longer frame lengths decrease the refresh rate at which synchronization is performed and hence power consumption and shorter frame lengths conversely invoke the opposite. TSMP does refrain from doing so because it requires long listening windows which consume power. Instead, TSMP nodes maintain a precise sense of time and exchange only offset information with neighbors to ensure alignment. These offset values are exchanged during active periods together with the usual data and acknowledgement packets hence invoking negligible overhead. TSMP nodes are active in three states: 1) sending a packet to a neighbor; 2) listening for a neighbor to talk; and 3) interfacing with an embedded hardware component. The duration of active periods, i.e. the duty cycling is very flexible in TDMA; typical applications require duty cycles of less than 1%. When applied, the sink typically retrieves the list of nodes, their neighbors and their requirements in terms of traffic generation. From this information, it constructs a scheduling table in both time and frequency. When implementing TSMP on IEEE 802.15.4 compatible hardware, 16 frequency channels are available. Exemplified by means of the scheduling table of Fig. 3, the TSMP link establishment and maintenance rules are simple:

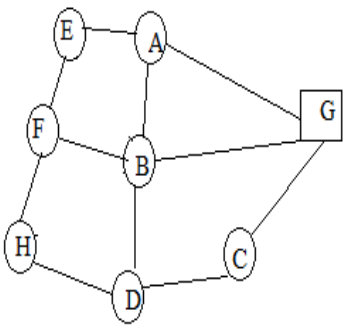

Fig.3.A. connectivity graph.

Ch15										
Ch14	A-G			G-C					E-A	

Ch13						D-H				
Ch12		F-E					B-A			
Ch11					C-D					F-B
Ch10			G-B							
Ch09										
Ch08	E-F					G-A		B-G		
Ch07				D-B						A-E
Ch06					H-F					
Ch05		D-C					C-G			
Ch04									B-D	
Ch03										
Ch02	H-D					B-F				
Ch01			F-H							
Ch00					A-B					

t1 t2 t3 t4 t5 t6 t7 t8 t9 t10

Fig.3B.Possible schedule for given connectivity graph.

Never put two transmissions in the same time/frequency slot; at a given time, a given node should not receive from two neighbors nor have to send to two neighbors. Assuming that slots are 10ms long and node *H* sends a packet following route $H \rightarrow F \rightarrow B \rightarrow G$, then *H* send to *F* in slot [t5, ch.6], thereafter $F \rightarrow B$ in [t10, ch.11], then $B \rightarrow G$ at [t8, ch.8]. Latency is hence in this particular case 13 slots (130ms) and in general always guaranteed to be bound by a finite value which depends on the particular design of the time frequency pattern.

V. Distributed Scheduling

By using a local scheme, the drawback of transmitting information to a central node and getting back slots assignment is avoided. SMACS (Self-organizing Medium Access Control for Sensor networks) [28] allows nodes to establish a communication infrastructure between neighboring nodes by defining transmission and reception slots. SMACS is localized and distributed, that is, there is no need for a master node. It contains two phases: neighbor discovery and channel assignment. In SMACS, a channel is assigned to a neighbor if discovered. Each link works on a different channel, i.e. a different frequency randomly chosen from a given set, to reduce collisions. To find its neighbor, a node wakes up and listens for a given time to receive invitation packets. If it does not receive such a packet, it starts inviting others by sending an invitation packet. To save energy, nodes sleep and wake up randomly. There is, however, a non-vanishing probability that two nodes never meet. When a link is formed between two nodes, they establish transmission-reception slots. These slots are used periodically to exchange data between nodes. Outside these slots, nodes sleep to save energy. The advantage of this method is that it is simple to implement, because slots are formed on the fly. The drawbacks are: the energy consumption, the low degree of connectivity of the network, and the difficulty of finding optimal routes. Furthermore, broadcast is not naturally supported since replaced by a series of unicast packets.

VI. Conclusion

In this paper, we explore the problem of the optimal WSN deployment, with an objective of minimizing the network cost with lifetime constraint. We discuss and identify the characteristics of a type of WSN applications and algorithms. The ultimate objectives of the device deployment for such applications are presented and discussed. We refine a deployment problem in a practical and fundamental scenario and its algorithms. We model this problem with the minimum set covering problem. Based on a recursive algorithm, a deterministic deployment strategy is proposed.. Furthermore, no MAC as of today is proven to be highly scalable as well as facilitate network ramp-up and auto organization/configuration/healing. This is particularly of importance,when sensor nodes arrive in a box of several thousands of nodes and are being switched on for deployment. Since this large quantity of nodes are within their one-hop radio neighborhood, any MAC described above will experience serious operational problems. On the deployment side, in the future, less nodes will really be equipped with batteries. It is expected that the majority of the WSN nodes will be relying on power harvesting. This has a profound impact on the MAC design, including its schedules. For instance, if power can be harvested every 24h only, then the MAC protocol needs accordingly be adapted to provide a high activity level during the time the node is energized.

REFERENCES

[1] D. Yupho and J. Kabara, "The Effect of Physical Topology onWireless Sensor Network Lifetime," Journal of Networks, vol. 2,September, 2007 2007.
[2] Q. Jiang and D. Manivannan, “Routing protocols for sensor networks,” in Proc. IEEE CCNC,Jan. 2004.
[3] G. ´Acs, L. Butty´an, and I. Vajda. The security proof of a link-state routing protocol for wireless sensor networks. In Proceedings of the 3rd IEEE Workshop on Wireless and Sensor Networks Security (WSNS 2007), 2007.

[4] G. ´Acs and L. Butty´an. Secure routing in wireless sensor networks. In Wireless Sensor Network Security (Cryptology and Information Security Series), Eds. J. Lopez and J. Zhou.ISBN: 978-1-58603-813-7, IOS Press, 2008.
[5] Wood, A. and Stankovic, J. A., (2020) "Denial of Service in Sensor Networks", IEEE Computer, 35(10):54-62, pp. 54-62.
[6] Intanagonwiwat, C., Govindan, R. &Estrin, D., (2003) "Directed Diffusion for WirelessSensor Networking", IEEE/ACM Transaction on Networking, VOL. 11, NO. 1.
[7] Siahaan, I. and Fernandes, L. (2008), "Secure Routing in Wireless Sensor Networks",University of Trento.http://dit.unitn.it/~fernand/downloads/IWSNSlides.pdf
[8] Anthony D. Wood, John A. Stankovic, Gang Zhou, "DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks," in The 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), San Diego, CA, June 2007.
[9] Wenliang Du and Jing Deng, " A Pairwise Key Pre- Distribution Scheme for Wireless Sensor Networks," Conference on Computer and Communications Security archive Proceedings of the 10th ACM conference on Computer and communication security table of contents Washington D.C., USA, Pages: 42 – 51, 2011.

About the author

M.Chithik Raja MSc.,M.E.(PhD)., He has finished his Master Degree in M.S.S.Wakf Board College at Madurai. Master of Engineering is awarded by Anna University Chennai Affiliation, Tamilnadu. Now He is pursuing his research in Wireless Sensor Network Security and System Architecture. He has written more than 10 Reputed International Journal and Conference Proceedings. He has published 3 International Standard Academic Books. He has more than 11 years of Academic Experience in International level Technological College as well as University. He is font of conducting workshop and writing Books for Recent Communication Technologies and System ArchitectureinWireless sensor Networks..