POWER AWARE ROUTING FOR MOBILE AGENT IN AD-HOC NETWORKS

[1]S ARVIND, [2]DR.T.ADILAKSHMI
[1]Department of Computer Science & Engineering, Guru Nanak Dev Engineering College, Bidar – 585 401
[2]Department of Computer Science & Engineering, Vasavi College of Engineering, Hyderabad- 500031

Email: scarvi@rediffmail.com, t_adilakshmi@rediffmail.com

ABSTRACT

Wireless networks allow a more flexible model of communication than traditional networks since the user is not limited to a fixed physical location. Unlike cellular wireless networks, an ad hoc wireless network does not have any fixed communication infrastructure. For an active connection, the end host as well as the intermediate nodes can be mobile. Therefore routes are subject to frequent disconnections. In such an environment, it is important to minimize disruptions caused by the changing topology for critical application such as voice and video. This presents a difficult challenge for routing protocols, since rapid reconstruction of routes is crucial in the presence of topology changes. By exploiting non-random behaviors for the mobility patterns that mobile users exhibit, we can predict the future state of network topology and perform route reconstruction proactively in a timely manner. Moreover, by using the predicted information on the network topology, we can eliminate transmissions of control packets and thus reduce overhead. This paper proposes a methodology of routing protocol for misbehaving network called RMP-ANT (Route Management Protocol for Ad Hoc Network) with a power management scheme called as MARI (Routing Intelligent Mobile Agent) protocol, and discusses about the various schemes to improve routing protocol performance by using mobility prediction. The protocol used here enables nodes to detect misbehavior by observing the status of the nodes. The paper also proposes distributed reputation system that can cope with false information and effective utilization of the power.

Keywords: *ad hoc networks, wireless networks, optimal routing, power management.*

1. INTRODUCTION

In wireless networks, networking grows rapidly because of the increase in the interest for mobility and freedom from limitation, i.e., from connection oriented communication networks [1]. Recent advances in wireless technology have helped the users to equip portable computers, like notebook computers and personal digital assistants with wireless interfaces for networked communication, thus making mobile ad hoc networks as a self organizing and rapidly deployable network in which neither a wired backbone nor a centralized control exists.

The network nodes communicate in a multi hop fashion with one another over wireless channels. The ad hoc network is adaptable to the highly dynamic topology resulted from the mobility of network nodes and the changing propagation conditions. Mobile ad hoc networks (MANET) are also a good alternative in rural areas or third world countries where basic communication infrastructure is not well established. Another interesting application of MANET's is ever-present computing [1]. Intelligent devices are connected with one another via wireless links and are self-organized in such a way that a newly joined node can request service from local servers without any human intervention. This leads to the analysis and implementation of wireless ad hoc networks for reliable communication.

In section 2, we discuss about ad hoc networks. Section 3 deals with power management in MANETS. Section 4 deals with misbehavior in ad hoc wireless networks. In section 5, we discuss about proposed power management and topology scheme. Section 6 deals with path management protocol in ad hoc networks and RMP-ANT protocol is discussed in section 7.

2. AD HOC NETWORKS

An ad hoc network is a collection of wireless nodes dynamically forming a network without using any predefined infrastructure. The goal of an ad hoc network is to enable communication between any two wireless connected nodes in the network. Communication between nodes that are beyond direct communication range is enabled by using intermediate nodes in the network as forwarding agents.

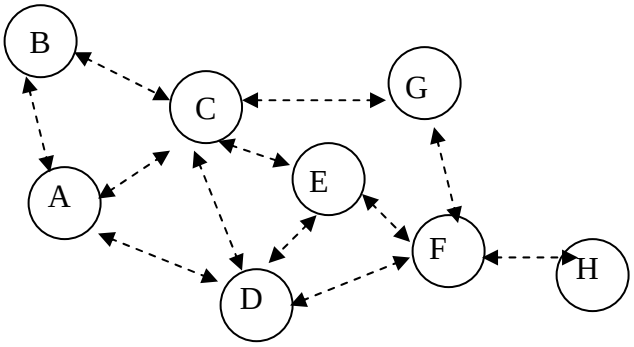

Figure 1. A wireless Ad Hoc Network

In ad hoc networks, each node acts as a router and most of the routes are multi hop. Nodes in these networks move arbitrarily, thus making network topology to change frequently, unpredictably, and may be with unidirectional links as well as bi-directional links. Each node in these networks operates on constrained battery power, which eventually get exhausted with time. Ad hoc networks are also more prone to security threats and misbehaving. All these limitations and constraints make Ad Hoc network research more challenging.

3. POWER MANAGEMENT IN MANET

Power management is an important technique to reduce the energy consumed in the wireless interface of battery-powered mobile devices. However, due to the nature of distributed coordination, energy saving and performance are inherently contradict in power-managed wireless networks. The design of optimal power management policies needs to explicitly account for the diverse performance requirements posed by different application scenarios such as latency, throughput and other performance metrics. Quantitative characterization of the energy-performance trade-off for different power management policies play an essential role in understanding, evaluating and devising better power management protocols.

With the proliferation of portable computing platforms and small wireless devices, wireless networks have received more and more attention as a means of data communication among devices regardless of their physical locations.

As wireless devices usually rely on portable power sources such as batteries to provide the necessary power, power management in wireless networks has become a crucial issue. It has been observed that energy is not only consumed by the active communication in wireless networks, but also consumed in idle state. Experimental results have shown that the energy consumed by wireless devices in the idle state is only slightly less than what they consume while they are at transmitting or receiving states [2]. As a result, an important technique to reduce power consumption in wireless networks is to place nodes in the low-power sleep state whenever possible.

Power management techniques have been studied extensively in the context of CPU, memory and disk management in the past. The main idea is to switch devices to the low-power state in periods of inactivity. As compared with traditional techniques in operating systems, power management in communication devices requires distributed coordination between two (or multiple) communicating entities, as all the entities have to be in the active mode for a successful communication. When the arrival pattern of communication events is not known a priori, communication over the same wireless channel is required to inform a remote sleeping node to wake up for packets destined for it. This makes power management seemingly simpler. For example, if node A has packets destined for node B while node B is in the low-power state, node A has to wait till node B becomes active before it transmits any packet. On the other hand, when node B is in the low-power state, it has no idea that node A has packets destined for it. Therefore, energy saving and performance inherently contradict each other in power-managed wireless networks. A naive design that minimizes the energy consumption may render the network non-operational.

This paper proposes a plan to present an analytical characterization of energy consumption, delay and loss rate of power management policies as a function of the traffic load, buffer size and protocol specific

parameters. To facilitate abstraction without loss of generality, the traffic-dependent power management schemes can be categorized into polling based and time-out driven policies. By proposing a theoretical model to analyze the time-out driven policies based on a variation of M/G/1/K queuing system with multiple vacations. The aim of this paper is to find the best power management policy that exhibits a threshold structure, i.e., when the traffic load is below certain threshold, a node should switch to the low-power state whenever possible and otherwise remain awake.

For polling based policies, this paper proposes the use of IEEE 802.11 power saving mode (PSM) as an example and model the effect of the length of beacon intervals on the performance. The analytical results must produce the dynamic tuning of beacon intervals with a marginal impact on energy consumption, while the average delay can be significantly higher in the case of large beacon intervals. That is, IEEE 802.11 PSM should not provide a rich set of control knobs to achieve a good balance between energy and other performance metrics, and additional control variables should be devised for better power management.

A power management policy in wireless networks is invoked to make the following decisions: i) which set of nodes should perform power management, ii) when a power-managed node switches to the low-power state and iii) when a power-managed node switches from the low-power state to the active state.

In wireless networks, the first decision depends upon the location and/or the hardware capability of the wireless node. For example, in wireless LANs, base stations are usually wall-powered and thus energy is not an issue while battery-powered mobile devices should be put to the low-power state whenever possible. In multihop wireless networks, the power management decision can be location-dependent. **GAF** [3] uses geographical information to divide all the nodes into grids and delegates one leader node to remain on in each grid. Span [4] uses a distributed scheme to elect coordinates with the goal of maintaining connectivity and capacity of the network.

The second and third decisions for a power-managed node have to take into account of traffic characteristics. For example, a node should always stay in the low-power state when no active communication takes place in order to conserve energy. Depending on how the decision is made to switch from the active state to the low-power state, power management policies can be categorized into two groups, i.e., i) polling based and ii) time-out driven.

In polling based power management policies, a node polls other nodes periodically (or equivalently makes announcement to other nodes) to decide whether or not it (or the others) should remain active. One example of this type of policies is IEEE 802.11 power saving mode (PSM). In the IEEE 802.11 specification, all nodes in the network are synchronized to wake up periodically in every beacon interval. To send a broadcast/multicast packets or unicast packets to a power-saving node, an announcement is made via **a t**raffic **i**ndication packet(ATIM) at the beginning of the beacon interval called the **ATIM** window. If a node receives an ATIM frame destined for it during the ATIM window, it sends an acknowledgment and stays awake for the entire beacon interval waiting for data packets to be transmitted. Clock synchronization is needed to coordinate power management states of nodes. Broadcast/multicast packets announced in the ATIM window need not be acknowledged. Immediately after the ATIM window, nodes can transmit buffered broadcast/multicast frames, data packets and management frames destined for nodes that have acknowledged a previously transmitted ATIM frame. Following the transmission of all buffered data packets, nodes transmit packets destined for receivers that are known to be in the active state for the current beacon interval.

In time-out driven power management policies, switching to the low-power state is triggered by a prolonged period of inactivity (usually implemented as a time-out event). In multihop wireless networks, several time-out based schemes have been proposed. **STEMM** [5] uses asynchronous beacon packets in a second control channel to wake up intended receivers. After transmissions have ended (e.g. after a time-out), the node turns its radio off in the data channel. In S-MAC, a mechanism called packet passing is proposed that modifies a network allocation vector (NAV) for virtual channel reservation in protocols of the IEEE 802.11 MAC type. The length of the NAV is determined by the duration of a burst of packets. The virtual reservation serves two purposes: (1) it mandates the receiver to remain on throughout the transmission of the burst, and (2) it prevents other nodes from transmitting in this interval.

One common feature of both types of power management policies is that energy can be saved by turning the interface to the low-

power state when it is not actively transmitting or receiving packets. However, the characterization of energy consumption, delay and loss rate as a function of the traffic load is quite different for various power management policies.

A good power-saving topology management scheme for wireless ad hoc networks should have the following characteristics:

- It should allow as many nodes as possible to turn their radio receivers off most of the time because even an idle radio in receive mode can consume almost as much energy as an active transmitter.
- It should forward packet between source and destination with minimally more delay than if all nodes were awake. This implies that enough nodes must stay awake to form a connected backbone.
- The algorithm for picking this backbone should be distributed, requiring each node to make a local decision.

To fulfill the above requirements, we have designed a topology management scheme for ad hoc wireless networks must be designed where in each node in the network makes periodic, local decisions on whether to sleep or stay awake and as a MARI node, participate in the forwarding backbone topology. A node volunteers to be a MARI node if it discovers, using information it gathered from local broadcast messages, that the node has maximum power level among its one hop neighbors. MARI nodes select its Gateways thus ensuring a connected backbone.

4. MISBEHAVIOUR IN AD HOC WIRELESS NETWORKS

In mobile ad hoc networks, nodes are both routers and terminals. For lack of routing infrastructure, they have to cooperate to communicate. Cooperation at the network layer means finding a path for a packet, and forwarding, i.e., relaying packets for others. Misbehavior means deviation from regular routing and forwarding. It arises for several reasons, non-intentionally when a node is faulty. Intentional misbehavior can aim at an advantage for the misbehaving node or just constitute vandalism, such as enabling a malicious node to mount an attack or a selfish node to save power. In game-theoretic terms, cooperation in mobile ad hoc networks poses a dilemma. To save battery, bandwidth, and processing power, nodes should not forward packets for others. If this dominant strategy is adopted, however, the outcome is a non-functional network when multi-hop routes are needed, so all nodes are worse off. Without countermeasures, the effects of misbehavior have been shown to dramatically decrease network performance.

Depending on the proportion of misbehaving nodes and their strategies decrease in network throughput, packet loss, denial of service and network portioning may occur. These detrimental effects of misbehavior can endanger the entire network. Unless misbehavior is addressed to provide reliable and trustworthy ad hoc networks, users might be reluctant to use them. Mobile ad hoc networks do not rely on any fixed infrastructure but communicate in a self-organized way. Their properties lead to new vulnerabilities to attacks unknown in infrastructure-based or wired networks. This paper addresses these requirements for more fairness and robustness of mobile ad hoc networks. One of the protocols presented and discussed in the MANET working group of the IETF is the Dynamic Source Routing (DSR) protocol. An extension to DSR is planned in this paper. The lack of infrastructure and organizational environment of mobile ad hoc networks offer special opportunities to attackers. Without proper security, it is possible to gain various advantages by malicious behavior: better service than cooperating nodes, monetary benefits by exploiting incentive measures or trading confidential information; saving power by selfish behavior, preventing someone else

5. PROPOSED POWER MANAGEMENT AND TOPOLOGY SCHEME

Minimizing energy consumption is the important challenge in mobile networking. Wireless network interface is often a device's single largest power consumer. Since the network interface may often be idle, turning the node off when not in use could save a considerable amount of power. In practice, however, this approach is not straightforward. A node must arrange to turn itself on not just to send packets, but also to receive packets addressed to it and to participate in any higher-level routing and control protocols. The requirement of cooperation between power saving and routing protocols is particularly acute in the case of multi-hop ad hoc wireless networks, where nodes must forward packets for each other.

In the proposed topology management scheme, MARI nodes are to be selected in such a way that MARI nodes have the maximum power level among their on hop neighbors and all non-MARI nodes are within the transmission range of MARI nodes. These MARI nodes have the routing intelligence i.e. they make all decisions related to routing. The Gateway nodes having sufficient power level are selected so that they can forward packets between MARI nodes. Gateway nodes do not have routing intelligence. These MARI and Gateway nodes stays continuously awake to route the packets of other member nodes. The member nodes wake up a number of times in a beacon period T, and if they do not have to transmit or receive data, they go to sleep mode again. The wake up time for each node is calculated from a pseudo-random number, such that MARI node and neighbor nodes know the wake up time of that node .Thus the member node can remain in power saving sleep mode most of the time, if it is not actively sending or receiving packets. The packets are routed over the virtual backbone consisting of MARI nodes and Gateways. The routes are found with the help of mobile agents.

The topology management scheme runs above the MAC layer and interacts with the routing protocol. If a node has been asleep for a while, packets destined for it are not lost but are buffered at a neighboring MARI node. When the node awakens, it can retrieve these packets from the buffering MARI node. This topology management schemes makes the routing simple, as only those entries in a node's routing table that correspond to currently active MARI nodes can be used as valid next-hops (unless the next hop is the destination itself).

We assume that each node periodically broadcasts WAKEUP messages that contains:

- Node's id,
- status (i.e., whether the node is a MARI node, Gateway, member, or undecided),
- current POWER level,
- current MARI node,
- A wakeup counter wi,
- Information about each neighbor i.e.
    - Neighbors id,
    - status
    - MARI node.

Based on the WAKEUP messages received from neighbors, each node constructs a list of it's neighbors, their MARI nodes, POWER level, wakeup counter and information about their neighbors.

A node must switch its state from time to time between being a MARI node and being a member. A node becomes a Gateway, if its MARI node chooses it as a Gateway to route the packets between MARI nodes. It has to switch its state to undecided, if it looses contact with its MARI node due to mobility.

6. PATH MANGEMENT SCHEME

This paper proposes a Path Management protocol in Ad Hoc Network (RMP-ANT) to cope with misbehavior. In this approach RMP-ANT protocol is used in detecting misbehaving nodes and to isolate them from the network, so that misbehavior will not pay off but result in denied service and thus cannot continue. RMP-ANT detects misbehaving nodes by means of direct observation or second-hand information about several types of misbehavior, thus allowing nodes to route around these misbehaving nodes and to isolate them from the network.

In the proposed approach each node has a monitor for observations, reputation records for first-hand and trusted second-hand observations about routing and forwarding behavior of other nodes, trust records to control trust on received second-hand information, and a path manager to adapt their behavior according to reputation and to take action against misbehaving nodes.

In the RMP-ANT protocol each node monitors their neighbors and change their reputation accordingly. From time to time they must exchange the first-hand information obtained by monitoring with other nodes, for potential consideration in the reputation system. If they have reason to believe that a node misbehaves, i.e. when the reputation rating is bad, they must take action in terms of their own routing and forwarding by routing around suspected misbehaving nodes. Depending on the rating and the availability of paths to the destination, the routes containing the misbehaving node are either re-ranked or deleted from the path cache. Future requests by the badly rated node are to be ignored. Detection, reputation, and response system schemes aim at reactively detecting misbehavior and proactively isolating misbehaved nodes to prevent further damage.

7. RMP-ANT PROTOCOL

In RMP-ANT protocol each node monitor their neighborhood and detect several kinds of misbehavior by means of an enhanced passive acknowledgment mechanism designed. This means that every time a node sends a packet, it listens to overhear whether the next-hop node on the route forwards the packet correctly.

Consider the following scenario as depicted in Figure 2.

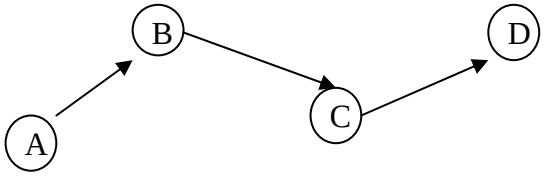

Figure 2. Packet forwarding between nodes

Node A sends packets via nodes B and node C to the destination D. For every packet, nodes keep track of the behavior of the next-hop node and remember whether it has forwarded the packet correctly. Node A stores ratings about node B, node B about node C, etc., which is called as first-hand information, since the ratings are derived from direct observation. Suppose that node C misbehaves by dropping the packet instead of forwarding it, as shown in Figure 3, node B rating of node C then becomes bad. Since A is not in range with C, it cannot directly observe its behavior and thus cannot find out about C's misbehavior.

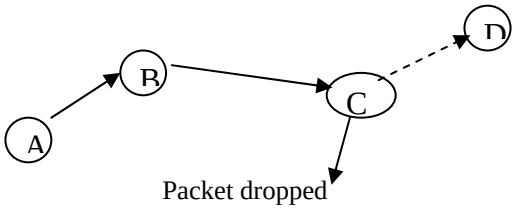

Figure 3. Packet dropping at node C.

We can solve this problem by using second-hand information as follows. In addition to keeping track of direct observation, nodes publish their first-hand information from time to time by local broadcasts to exchange information with other nodes. This information is termed as second-hand information. Node A thus receives information from its neighbor node B about node C. Again, since node A has no first-hand information about node C, it can only find out about node C's misbehavior by second-hand information. There is, however, a problem since second-hand information can be false. Node A could for instance make false accusations about another node.

In this paper a combination of two mechanisms to cope with spurious second-hand information is being proposed. Firstly, we can consider second-hand information that is not incompatible i.e. that does not deviate too much from the reputation rating. The motivation behind this is, that when second-hand information deviates substantially from the rating a node has built over time using previously received second-hand information from several sources and potentially its own first-hand information, it is more likely to be false. Secondly, even when second-hand information is compatible, it is allowed to slightly influence the reputation rating.

Nodes must use the reputation ratings that they keep about other nodes to classify them. This classification provides a basis for decision making about providing or accepting routing information, accepting a node as part of a route, and taking part in a route originated by some other node. Nodes classify other nodes as misbehaving if their reputation rating is worse than their threshold for misbehavior tolerance. Once a node classifies another as misbehaving, it isolates that node from the network by not using it for routing and in turn not allows the node to be used later.

8. CONCLUSIONS

In this paper we discussed the need to make routing protocols power-aware. This paper proposed a methodology of routing protocol for misbehaving network called RMP-ANT with a power management scheme called as MARI protocol, and discussed about the various schemes to improve routing protocol performance by using mobility prediction. The protocol used here enables nodes to detect misbehavior by observing the status of the nodes. The paper also proposes distributed reputation system that can cope with false information and effective utilization of the power.

REFERENCES

[1]. Chen W., Jain N., and Singh S., ANMP: Ad Hoc Network ManagementProtocol, IEEE Journal on Selected Areas of Communications, vol. 17, no. 8, pp.1506-1531, August 1999.

[2]. Kravets, R., & Krishnan, P., Application driven power management for mobile communication, Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Dallas TX US, pp.263.-277, 2000.

[3]. Shen C., Srisathapornphat C, and Jaikaeo C., An adaptive management architecture for ad hoc networks, IEEE Communications Magazine, vol. 41, no.2, pp. 108-115, February 2003.

[4]. Tamer A. ElBatt, Srikanth V. Krishnamurthy, Dennis Connors, and Son Dao, Power management for throughput enhancement in wireless ad-hoc networks, in IEEE International Conference on Communications, 2000.

[5]. M. Stemm and R. H. Katz, “Measuring and reducing energy consumption of network interfaces in hand-held devices,” IEICE Transactions on Communications, vol. E80-B(8), pp. 1125–1131, August 1997.

.