Passive and Active Hidden Terminal Detection in 802.11-based Ad Hoc Networks

Frank Y. Li*, Arild Kristensen*, and Paal Engelstad**
*University Graduate Center, University of Oslo, N-2027, Kjeller Norway
**Telenor R&D, PO Box 1331, Fornebu, Norway
Email: *{frank.li, arildkri}@unik.no; **paal.engelstad@telenor.com

***Abstract*—To *preventively* detect hidden terminals in a node's vicinity, two detection mechanisms, referred to as passive detection and active detection, are proposed and compared in this poster. Simulations based on IEEE 802.11-based ad hoc networks are carried out to evaluate the proposed schemes.**

***Index Terms*—ad hoc networks, hidden terminal, passive detection, active detection, simulation.**

I. INTRODUCTION

Various kinds of mechanisms have been proposed to lessen or eliminate the effect of hidden terminals. The most well known one is probably the four-way frame exchange protocol [1] adopted by the IEEE 802.11 standard [2], where two optional frames, RTS and CTS are exchanged before each DATA and ACK transmission. From our understanding, this four-way handshake represents only a *proactive and pre-emptive* solution for hidden terminal elimination, in the sense that the RTS/CTS packets are exchanged no matter whether there is a hidden terminal in the vicinity or not.

However, using RTS/CTS can be costly in terms of bandwidth consumption, and using it in situations where there are actually no hidden terminals, is wasteful. Moreover, as pointed out by many recent papers, e.g., [3-4], the problem of hidden terminals still remains more or less unsolved by employing the RTS/CTS mechanism.

Therefore, a better solution would be a *preventive* mechanism where a node knows explicitly whether there are hidden terminals or not. The RTS/CTS mechanism is consequently used only when necessary. Hidden terminal detection is the mechanism to obtain the knowledge of hidden terminals in a node's vicinity. This issue is the main focus of this study.

Even though hidden terminal detection is currently under discussion within the 802.11k (TGk) group of the IEEE [5], this topic has not received much attention in the ad hoc network research community at large. Furthermore, the solution proposed in 802.11k is what we refer to as "receiver-initiated". We argue that this method is not very suitable for ad hoc networks, where a "sender-initiated" detection scheme is preferable.

In this poster, we propose to use a passive and/or an active mechanism to detect hidden terminals in 802.11-based wireless networks, depending on different situations. After describing the detection principles, we conduct a series of simulations to evaluate the effectiveness and verify the appropriateness of these two mechanisms. The pros and cons of each mechanism are also discussed.

II. HIDDEN TERMINAL DETECTION

A. Initiation of Hidden Node Detection

The detection of hidden terminals can be initiated either by the receiver or the sender of the potentially colliding packets. If a node wants to avoid collisions of traffic it is receiving, it initiates detection of its neighbors that are hidden to each other. This is referred to as "receiver-initiated" detection. On the other hand, if a node wants to avoid collision of traffic it is sending, it initiates detection of two-hop neighbors that are hidden to it. This is referred to as "sender-initiated" detection.

The "receiver-initiated" detection is particularly designed in 802.11k. This scheme fits well to the infrastructure mode where all traffic within a BSS goes between the AP and the other stations, and no nodes in the BSS are hidden to the AP. Thus, all collisions due to hidden nodes will happen at the AP. In this situation, it makes sense that the AP observes the possibilities for collisions of traffic it is receiving from hidden node pairs amongst its neighbors, and determines whether or not RTS/CTS should be used within the BSS.

In ad hoc networks, however, collision due to hidden terminals can occur at any node in the network, and the need for RTS/CTS protection may vary from situation to situation. Due to bandwidth scarcity in wireless networks, eliminating unnecessary use of RTS/CTS can be beneficial. We argue therefore that the "sender-initiated" solutions would often be preferable in ad hoc networks.

B. Detection Mechanisms for Ad Hoc Networks

In the context of sender-initiated hidden terminal detection, a node that wishes to perform hidden terminal detection is hereafter referred to as a *detecting node*. Two detection mechanisms are presented in this subsection: passive detection and active detection. The detailed descriptions of the mechanisms and discussions on parameter settings in detection are omitted here due to the 3-page limit.

1) Mechanism I: Passive Detection. Passive detection is only possible when there is ongoing traffic exchange between the detecting node's one-hop neighbors and the potential hidden terminals of the detecting node. With passive detection, a detecting node does not generate any traffic itself, but solely relies on monitoring the ongoing traffic in the neighborhood to obtain the picture of its hidden terminals. The

only requirement for conducting passive detection is that the detecting node has to be set in the *promiscuous* mode in which all packets, regardless of destinations, are processed by the detecting node.

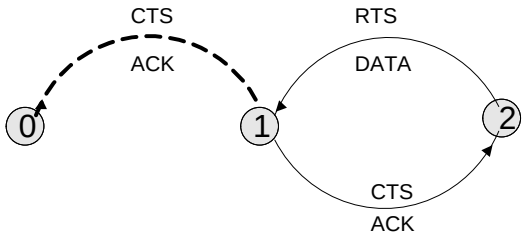

Figure 1. Passive detection – with RTS/CTS enabled.

There are two different cases of passive detection, depending on whether RTS/CTS is being used or not. Only the one where RTS/CTS is enabled is discussed here. In Figure 1, node 2 is attempting to send DATA packets to node 1. The detecting node, node 0, can only hear the CTS and the ACK frames sent by node 1, which are supposed to arrive after the RTS and DATA frames. Based on this information, node 0 concludes that node 2 is a hidden terminal to it and extracts the MAC address of the hidden terminal from the CTS or ACK frame. If the background traffic on the contrary is initiated from node 1 and destined at node 2, the hidden terminal can also be detected in a similar way. In this case, however, the detecting node receives the RTS and DATA packets, not the CTS and ACK frames.

2) Mechanism II: Active Detection. Active detection is the only workable option if there is no ongoing background traffic in the detecting node's neighborhood.

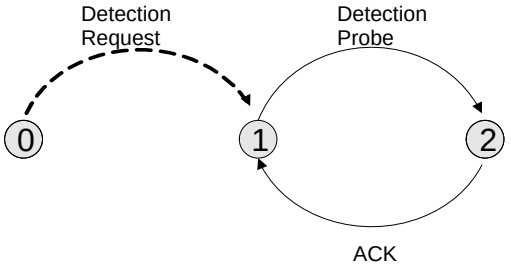

Figure 2. Active detection via detection request and probe.

Figure 2 illustrates the active detection mechanism, where node 0 is the detecting node. Two new types of packets, referred to as 'detection request' and 'detection probe' packets, have been introduced. With active detection, each node that wishes to know its potential hidden terminals will actively generate a detection request to all its one-hop neighbors. All neighboring nodes that receive this request will then start sending a sequence of unicast probe packets to their neighbors, for a time interval specified by the detection request. The detecting node will then perform measurements on the traffic generated by the neighbors. Based on the received packets, the detecting node is able to establish a complete list of its all hidden terminals, including those that may not be discovered by passive detection. The difference from passive detection is that the active detection procedure is triggered by the detecting node itself. Other operational procedures, such as receiving in the promiscuous mode and performing address extraction, are basically the same as for the passive detection mechanism.

3) Passive Detection versus Active Detection. The advantage of using the passive detection mechanism is that no extra protocol overhead is introduced. It might for example be a useful way of maintaining the hidden terminal list, which contains all the discovered hidden terminals. However, since passive detection might not be able to detection all the hidden terminals, active detection may be required now and then to reconstruct an exhaustive list of hidden terminals. Because active detection introduces additional protocol overhead, it might often make sense to limit the usage of active detection, and complement it with passive detection.

The amount of extra overhead introduced by active detection depends on the situation. For a stationary ad hoc network, each node, either the detecting node or the other involved nodes, needs only to generate dozens of packets. For a mobile ad hoc network, especially with high mobility, active detection is required more frequently, in order to get a timely picture of all hidden terminals. If all nodes in an ad hoc network require the knowledge of hidden terminals, the additional traffic of active detection is expected to be noticeable. Therefore, there is a tradeoff between using active detection on the one hand, and using RTS/CTS under all circumstances (i.e., without the need for hidden terminal detection at all), on the other hand.

III. SIMULATION SCENARIOS AND RESULTS

Three sets of simulations for hidden terminal detection are carried out using ns2 with some code modifications. The data rate is set as 11 Mbps, and the transmission range and the sensing range are deliberately set to the same value of 200 meters, to eliminate any possible effect of the sensing range. For the other parameters, the default values in ns2 are used.

A. Simulation Set I – Passive Detection

The goal of this set of simulation is to verify whether a node can passively detect any, and possibly all, potential hidden terminals around itself. Figure 3 shows a static network topology used in the simulations, with five stationary nodes located in a two dimensional area. The distances between nodes are specifically configured so that any pair of nodes that are separated by two hops are hidden terminals to one another.

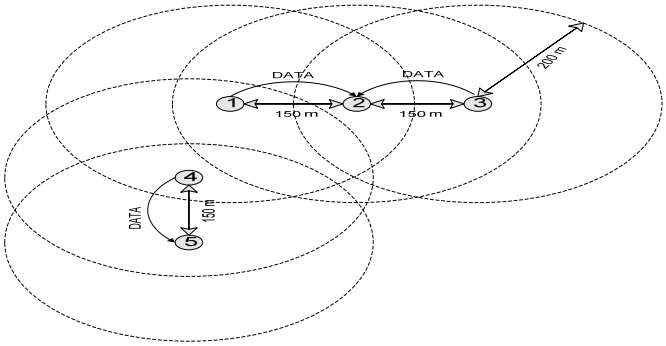

Figure 3. A static ad hoc network with 5 nodes.

As background traffic, three flows are generated by nodes 1, 3 and 4 respectively, and destined to nodes 2, 2 and 5 correspondingly. All three flows are UDP sessions sent at a constant bit rate of 59 Kbps with a packet length of 350 bytes. Two variations of the passive detection mechanism, with and without RTS/CTS, are studied separately. The obtained detection results are identical using both mechanisms, as listed below.

Table 1. Hidden terminal reports for passive detection.

Node	One-hop neighbor	Hidden terminal report
1	2, 4	3, 5
2	1, 3	No hidden node observed
3	2	1
4	1, 5	2
5	4	No hidden node observed

B. Simulation Set I I – Active Detection

The above obtained hidden terminal lists are obviously not exhaustive. Therefore active detection is activated. In our simulation, the lengths of the detection request packet and the detection probe packet are empirically set as 100 bytes and 60 bytes respectively. Upon receiving any request packet from a detecting node, the requested node generates a sequence of 20 probe packets, at an interval of 50 ms.

The simulation scenario for active detection is the same as the one for passive detection, except that the ongoing packets are request and probe packets in this case. Table 2 shows the simulation results for active detection for all nodes in Figure 3. All hidden terminals are detected in this case.

Table 2. Hidden terminal reports for active detection.

Node	One-hop neighbor	Hidden terminal report
1	2, 4	3, 5
2	1, 3	4
3	2	1
4	1, 5	2
5	4	1

C. Simulation Set III – Detection for Mobile Nodes

The mobile scenario is depicted in Figure 4, with 3 fixed nodes (nodes 1, 2, and 3) and 1 mobile node (node 4). The detection is performed on the mobile node which is traveling across the network. Only results with passive detection are presented for this scenario. There are two ongoing CBR/UDP sessions, one from node 1 to node 2 and another from node 3 to node 2. The distances between nodes are specifically set so that node 4, which is moving from left to right at a constant velocity during simulation, is always within the reach of at least one of the other three nodes. The overall hidden terminal report for node 4 is illustrated in Figure 5, with the number of hidden nodes as y-axis and simulation time as x-axis. The result confirms that the detection mechanism works fine also for mobile nodes.

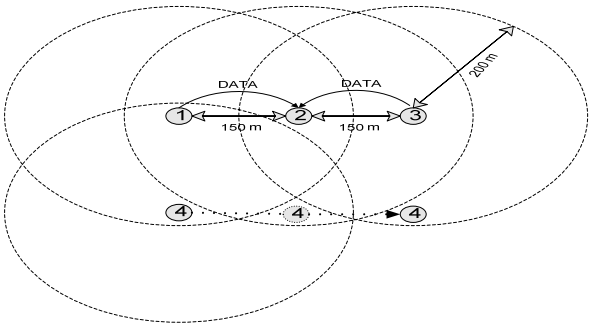

Figure 4. Hidden terminal detection for a mobile node.

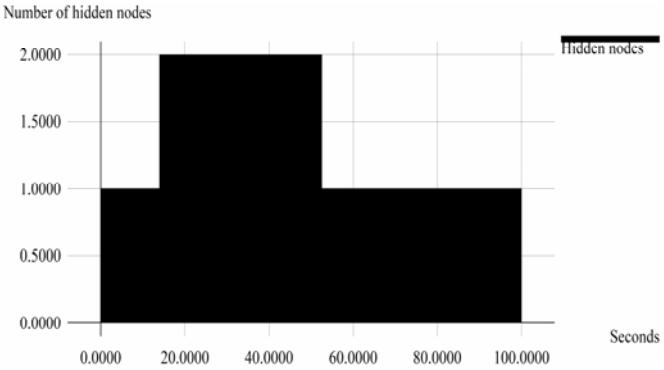

Figure 5. Hidden terminal report for the mobile node.

IV. Conclusions and Future Work

In this poster, we have presented and compared two hidden terminal detection mechanisms. The passive detection mechanism does not impose any extra traffic into the network, but it gives an incomplete picture of the potential hidden terminals. Active detection, on the other hand, reveals all potential hidden terminals of the detecting node, at a cost of extra bandwidth consumption by additional traffic generated. Optimization of parameters and the tradeoff mentioned in Subsection II.C need to be further investigated quantitatively.

Even though presented in the context of ad hoc networks, the proposed mechanisms can also be applied to BSS WLANs. Our proposal complements the 802.11k standardization effort, as it shows how the hidden terminal reports can be established at an AP or at any node in a wireless network.

References

[1] P. Karn, "MACA- A New Channel Access Method for Packet Rodio", Proc. ARRL/CRRL, Amature Radio Ninth Computer Networking Conf., pp. 134-140, 1990.

[2] IEEE Computer Society, "IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", International Standard ISO/IEC 8802-11: 1999(E), ANSI/IEEE Std 802.11, 1999 Edition.

[3] S. Ray, J.B. Carruthers, and D. Starobinski, "Evaluation of the Masked Node Problem in Ad-Hoc Wireless LANs", IEEE Trans. on Mobile Computing, vol. 4, no.5, pp. 430-442, 2005.

[4] J. L. Sobrinho, R. d. Haan, and J. M. Brazio, "Why RTS-CTS Is Not Your Ideal Wireless LAN Multiple Access Protocol ", in Proc. IEEE WCNC 2005.

[5] IEEE Computer Society, "Draft Amendment to Standard Amendment 7: Radio Resource Measurement", IEEE P802.11k/D1.0, July 2004.