Channel-Aware Detection of Gray Hole Attacks in Wireless Mesh Networks

Devu Manikantan Shila, Yu Cheng and Tricha Anjali
Dept. of Electrical and Computer Engineering,
Illinois Institute of Technology, Chicago, USA

***Abstract*—Gray hole attacks (a.k.a selective forwarding attacks) are a special case of denial of service (DoS) attack, where a misbehaving mesh router just forwards a subset of the packets it receives but drops the others. In wireless networks, it is particularly hard to detect the presence of such attackers because a packet loss over the wireless link can be due to bad channel quality, medium access collisions, or intentional dropping. In contrast to existing studies, we propose a more practical algorithm known as channel aware detection (CAD) that adopts two strategies, hop-by-hop loss observation and traffic overhearing, to detect the mesh nodes subject to the attack. We derive the optimal detection thresholds by analyzing the false alarm and missed detection probabilities of CAD. We also compare our approach to existing solutions and demonstrate that CAD detects the attackers effectively even in harsh channel conditions.**

I. Introduction

Multihop wireless mesh networks (WMNs) [1] are emerging as a promising solution to provision ubiquitous last-mile high-speed Internet access due to the advantages of scalability, self-management, and low up-front cost. However, compared to wired networks, the WMNs are more likely to suffer from various security attacks, due to the nature of open medium, distributed architecture and dynamic topology [1]-[3].

In this work, we focus our attention on the special case of denial of service (DoS) attack, known as *selective forwarding* attack (a.k.a *gray hole* attack) [2], [3]. With such an attack, the misbehaving router accepts the packet for transmission but refuses to forward certain packets by simply dropping them. Cryptography techniques are common approaches to protect the physically unprotected mesh routers from various DoS attacks, e.g., gray hole, black hole, sinkhole, and wormhole [2], [3]. Nevertheless, if the routers are compromised, the attacker will gain access to the public/private keys of the compromised routers and then break through the cryptographic systems. Therefore, non-cryptographic detection techniques offer a second line of defense. In this paper, we develop a non-cryptographic technique for detecting gray hole attack by monitoring and analyzing the forwarding behaviors of wireless mesh routers.

Most of the prior works [2]-[7] related to selective forwarding attacks were studied in the area of ad hoc and sensor networks. Karlof *et al.*[4] first proposed selective forwarding attacks and suggested that multi path forwarding can be used to counter these attacks in sensor networks. However, the algorithm fails to suggest a method to detect and isolate the attackers from the network. In [5], the authors propose a scheme that randomly selects part of the intermediate nodes along a forwarding path as checkpoint nodes which are responsible for generating acknowledgments for each packet received. If suspicious behavior is detected, it will generate an alarm packet and deliver it to source node. However, the algorithm suffers from high overhead because for each received packet the intermediate nodes need to send an acknowledgment back to the source node. Moreover, the authors also assumes that the channel is perfect and any packet loss is due to the presence of malicious nodes. In [6], authors propose Watchdog, a technique in which a node monitors its neighbors to determine whether they forward the packet to intended destination properly or not. The scheme fails to detect the attacker in presence of limited-transmit power attack, selective dropping attack and bad mouthing attack which can be addressed by the detection approach proposed in this paper. In BSMR [7], the authors propose a selective forwarding detection scheme for multicast routing protocols. However, BSMR assumes static detection thresholds which is independent of channel quality and medium access collisions.

While most of the previous studies [2],[3],[4]-[7], on selective forwarding attacks focus on attack detection under the assumption of an error-free wireless channel, we consider a more practical scenario that packet dropping may be due to an attack, medium access collision, or bad channel quality. In this paper, we propose a *channel aware detection* (CAD) approach that adopts two strategies, hop-by-hop loss observation and traffic overhearing. Each intermediary node in the forwarding path observes the behavior of its previous-hop and next-hop neighbors to detect the misbehaving nodes. These nodes judge the behavior of its neighbors by comparing the observations against two detection thresholds known as *monitoring* and *loss rate* threshold. In particular, the thresholds will be dynamically adjusted with the "natural" loss rates, due to bad channel quality and medium access collisions, to maintain the detection accuracy when network status changes.

The remainder of this paper is organized as follows. Section II describes the threat model and outlines the basic assumptions. Section III presents the proposed CAD algorithm. Section IV discusses how to estimate the normal loss rates due to channel quality and collisions. Section V computes the optimal detection threshold to minimize the sum of false alarm and missed detection probabilities. Section VI presents some simulation results to demonstrate the performance of CAD.

Yu Cheng's work was supported in part by NSF grant CNS-0832093

Section VII gives the conclusion remarks.

II. Threat Model and Assumptions

A. Threat Model

A gray hole attack forms a serious threat to mesh networks, particularly considering that collaboration among mesh routers is the basic requirement of such networks. An adversary may compromise these mesh routers through physical capture or software bugs, thus gaining full control of them. Once captured, the attacker gains access to all the data residing in victim node and reprogram them to behave in a malicious manner. For a path, $v_0, v_1, v_2, \ldots, v_n$, between the source S and destination D, we assume that node v_2 is a compromised router that attracts network traffic by advertising itself as having the high quality path to the destination and then performs selective forwarding attacks on the data passing through it. Suppose that source receives data from mesh client to forward to the destination D. On receiving the request for data transmission, it will check if it has an entry for node D in the routing table. If no entry is found, it will broadcasts a ROUTE REQUEST for that destination. Node v_2 claims that it has a better path to destination whenever it received ROUTE REQUEST packets and sends the reply back to source. The destination or other intermediate routers may send the reply if it has a fresh route to destination. If node S receives the reply from a *normal-behaving* node before it gets the reply from the attacker, everything works well. However, the ROUTE REPLY from v_2 can reach node S first for any of the following two reasons. (a) A malicious router may be near to the source router; (b) A malicious router does not have to check the routing table when sending false routing information. As a result, node S will think that the Route Discovery Phase is complete, ignore all other ROUTE REPLY packets and forwards data packets to D via v_2. Node v_2 will form a selective forwarding attack in the network by selectively dropping the subset of the packets it receives.

In this work, we focus on developing an algorithm that defends against *single* and *multiple* selective dropping attackers in WMN. In addition to gray hole attacks, we also address the following attacks such as limited transmit-power and bad mouthing attack.

B. Assumptions

We assume that the mesh nodes have no energy constraints and each mesh node is assigned with a public/private key pair and public keys of all other mesh nodes. These keys are used to protect the *packets* used in CAD design. Indeed, if a node is compromised, the attacker will gain access to the stored keys in that node. Hence, we argue that a combination of cryptographic and non-cryptographic solutions is necessary to achieve complete security in a network. CAD design further takes the following assumptions: (a) We trust only the source and the destination mesh nodes because the client device first authenticates with the mesh node before the forwarding sessions starts; (b) We consider a buffer of infinite size at each mesh node and hence, a packet can be dropped due to bad channel quality, medium access collision, or presence of an attacker; (c) Both the source and destination nodes are aware of the forwarding path and the ID's of each node in the path; (d) Since there are multiple routes from a source to a destination, a source may receive several route replies from a destination. We need the source node to cache these routes to mitigate the overhead incurred during new route discovery process. In this work, we mainly focus on the gray-hole attacks and thus we disregard general attacks such as sybil attacks, collision (or jamming) or node replication attacks. Furthermore, we only deal with the possibility of mesh nodes acting alone and hence, the problem of colluding nodes are not studied.

III. The Channel-Aware Detection Algorithm

In this section, we present a detailed design of *channel-aware detection* algorithm. The proposed CAD algorithm depends on two strategies, hop-by-hop loss observation and traffic overhearing, to detect the misbehaving nodes along a path. For a node v_i in a forwarding path, we refer to v_{i-1} and v_{i+1} as its *upstream* (previous hop) and *downstream* (next hop) nodes, respectively.

A. CAD Algorithm design

The essence of CAD is to identify intentional selective dropping from "natural" wireless losses. A "natural" packet loss can occur due to bad channel quality or medium access collisions under the infinite buffer assumption. These two types of loss events are independent and we present the estimation of "natural" losses (L) in sec. IV. In CAD, each mesh node maintains a history of packet count to measure the loss rate of the link. Therefore, when a node receives a packet from the upstream, it updates the packet count history with the corresponding packet sequence number and buffers the link layer acknowledgments (ACKs) received for each packet forwarded to downstream node. We denote the number of packets forwarded by source S to destination D as W_s and the number of packets received successfully by the intermediate node v_{i+1} from the upstream node v_i as $n^{v_i}_{v_{i+1}}$ over a time window. When a router forwards a packet to the downstream node, it performs two operations: (i) For each packet relayed to the downstream, it buffers the ACKs.[1] (ii) It also overhears the downstream traffic and determines whether the node *forwarded* or *tampered* the packet. Based on these observations, the node maintains two parameters for its downstream node, *probability of trust*, P_t and *probability of distrust*, P_{dt} where $P_t = 1 - P_{dt}$. The probability of distrust is computed as follows: $P_{dt} = \frac{n_t + n_d}{n_f}$. n_t and n_d are the number of packets tampered and dropped by the downstream node out of the total number of forwarded packets, n_f, respectively.

We introduce two new packets known as the PROBE packet and PROBE ACK packet for the detection of malicious routers. The source, S, sends a PROBE packet after every W_s data

[1]The ACKs serve as a proof for the successful relaying of traffic to the *downstream* node. To avoid the fabrication of the ACK packets, the nodes can digitally sign a portion of ACK packet (for e.g, sequence numbers).

packets. The smaller the value of W_s, the more likely the algorithm will detect the attackers faster. However, this means an increase in the overhead. On receiving the PROBE, each node in the path marks the PROBE packet with the detection parameters. This technique is known as *packet marking*. For each PROBE packet sent to destination, source marks the packet with the number of packets transmitted to the particular destination (W_s) and each intermediate node v_{i+1} marks the packet with the number of packets ($n_{v_{i+1}}^{v_i}$) it received successfully from its upstream node v_i. Additionally, when the packet is passed along the path, each node v_i also attaches a mark of its *opinion* to the downstream node v_{i+1}, denoted as $O_{v_i}^{v_{i+1}}$. It is computed by observing the downstream node's behavior by the transmitter.

$$O_{v_i}^{v_{i+1}} = \begin{cases} 1 & \text{if } P_{dt} > \tau_m; \texttt{[misbehaving]} \\ 0 & \text{if } P_{dt} < \tau_m; \texttt{[normal]} \end{cases}$$

where τ_m is the *monitoring* threshold and can take values between 0 and 1. As emphasized before, the main goal of CAD is to detect the attackers even in the presence of "natural" losses such as channel loss, collisions etc. Hence, in addition to $n_{v_{i+1}}^{v_i}$ and *opinion* parameters, each node except the source and destination appends the parameter $B_{v_{i+1}}^{v_i}$, the behavior. $B_{v_{i+1}}^{v_i}$ represents the observation of node v_{i+1} about the behavior of upstream node v_i and is computed by determining the packet loss rate of the link $\{v_i, v_{i+1}\}$ by the node v_{i+1}.

$$B_{v_{i+1}}^{v_i} = \begin{cases} 1 & \text{if } L_o^{v_i,v_{i+1}} > \tau_l; \texttt{[misbehaving]} \\ 0 & \text{if } L_o^{v_i,v_{i+1}} < \tau_l; \texttt{[normal]} \end{cases}$$

where $L_o^{v_i,v_{i+1}} = 1 - (n_{v_{i+1}}^{v_i} / n_{v_i}^{v_{i-1}})$ is the observed loss rate of link $\{v_i, v_{i+1}\}$. τ_l is the *loss rate* threshold and is computed as a function of $L^{v_i,v_{i+1}}$. τ_l can take any values between 0 and 1. The lower the values of τ_l and τ_m, the more likely the algorithm detects any malicious behavior. However, it also means that the probability of false alarm increases. Since each node individually monitors the behavior of its upstream and downstream neighbors in the path, CAD can also effectively detect *multiple single acting attackers* along the path.

For instance, assume that source S selects the path v_1, v_2, v_3 between the source and destination D. The PROBE message sent by the nodes in the forwarding path are:

$$S \xrightarrow{M} v_1 : M = S||\eta_S||W_S||O_S^{v_1}||MAC_S$$
$$v_1 \xrightarrow{M_1} v_2 : M_1 = M||v_1||n_{v_1}^S||O_{v_1}^{v_2}, B_{v_1}^S||MAC_{v_1}$$
$$v_2 \xrightarrow{M_2} v_3 : M_2 = M_1||v_2||n_{v_2}^{v_1}||O_{v_2}^{v_3}, B_{v_2}^{v_1}||MAC_{v_2}$$
$$v_3 \xrightarrow{M_3} D : M_3 = M_2||v_3||n_{v_3}^{v_2}||B_{v_3}^{v_2}||MAC_{v_3}$$

At each node, the message is attached with a message authentication code (MAC), which is generated with the node's private key and a nonce random number. The MAC signature can protect the message from being tampered and used in a replay attack. When destination receives the PROBE message, it first retrieves the ID of the last hop v_{i+n} and uses the corresponding public key to verify $MAC_{v_{i+n}}$. If $MAC_{v_{i+n}}$ is correct, it retrieves the ID of the upstream node of v_{i+n} and verifies the $MAC_{v_{i+n-1}}$. The destination node continues this process until *it has verified all* MAC's or *it finds an incorrect* MAC. Once all the MAC's are verified, destination D builds a list of suspicious nodes based on the detection parameters ($O_{v_i}^{v_{i+1}}$ and $B_{v_{i+1}}^{v_i}$) marked by each node in the forwarding path.

B. Attack Detection

1) Detection of Misbehaving Nodes: We consider the following scenarios where a node v_i is listed as suspicious by the upstream and downstream nodes.

Case A: $O_{v_{i-1}}^{v_i} = 1$ **and** $B_{v_{i+1}}^{v_i} = 1$. *node v_i dropped (or tampered) the packets:* In this case, node v_{i-1} will observe that v_i dropped (or tampered) the packets and increases n_d (n_t) for each packet dropped (or tampered). Node v_{i+1} also observes that the loss rate (L_o) of the link $\{v_i, v_{i+1}\}$ is greater than the threshold, τ_l. Hence in both cases, the nodes v_{i-1} and v_{i+1} set the detection parameters $O_{v_i}^{v_{i+1}}$ and $B_{v_{i+1}}^{v_i}$ to 1.

Case B: $O_{v_{i-1}}^{v_i} = 0$ **and** $B_{v_{i+1}}^{v_i} = 1$**.** (i) *limited-transmit power attack by v_i:* In this attack, node v_i could limit its transmission power such that the signal is strong enough to be overheard by the upstream node v_{i-1} although too weak to be received by the downstream node. Node v_{i-1} having observed that v_i forwarded the packet, increases the probability of trust (P_t) for v_i. The Watchdog scheme [6] relies on *downstream monitoring only* and can not detect such kind of attack. Nevertheless, with CAD node v_{i+1} by upstream monitoring will observe high loss rate L_o and sets $B_{v_{i+1}}^{v_i}$ to indicate the abnormal behavior of node v_i. (ii) *bad mouthing attack by node v_i:* In this case, node v_i falsely accuses that the loss rate of link $\{v_{i-1}, v_i\}$ is greater than the threshold value, τ_l, and sets $B_{v_i}^{v_{i-1}} = 1$. One way to get rid of this false accusation is to verify the link layer acknowledgments received by node v_{i-1} for each packet successfully forwarded to v_i.

Case C. $O_{v_{i-1}}^{v_i} = 1$ **and** $B_{v_{i+1}}^{v_i} = 0$**.** (i) *false report by node v_i:* In this case, node v_i falsely reports about the number of packets it received from the upstream node. For example, suppose that v_{i-1} forwarded 5 packets to v_i and v_i being a malicious node dropped 2 packets. The packet count at intermediate nodes v_i and v_{i+1} are $n_{v_i}^{v_{i-1}}$ = 5 and $n_{v_{i+1}}^{v_i}$ = 3. However, if v_i marks the PROBE packet with a value of 3 for $n_{v_i}^{v_{i-1}}$, node v_{i+1} will observe that L_o satisfies the threshold and hence assigns $B_{v_{i+1}}^{v_i}$ to 0. On the other hand, node v_{i-1} having observed the behavior of v_i increases the P_{dt} for each packet dropped and sets $O_{v_{i-1}}^{v_i}$ to 1. The link layer acknowledgments received by v_{i-1} can serve as a proof of successful relaying of traffic to v_i. Moreover, since the contents of PROBE packet are not hidden, v_{i-1} can also detect the misbehaving node v_i by observing the false information in PROBE packet.

2) PROBE ACK from Destination: CAD design require the destination to send a PROBE ACK message for every PROBE packet received from source.

(1) Negative PROBE ACK from D. In this case, the destination will send a PROBE ACK message to source, S,

with the list of suspicious router(s) based on the *opinion* and *behavior* parameters or on observing an incorrect MAC. It is to be noted that, similar to a PROBE message, the PROBE ACK message is also secured. When S receives the PROBE ACK message, it will query the suspicious routers for the proof of link layer acknowledgments. If a router is detected as misbehaving, source may use another path in route cache to forward the remaining data packets and informs the network about the attack to evict the misbehaving node. The details of node eviction is out of the scope of paper.

(2) Positive PROBE ACK from D. If no suspicious nodes are listed in the PROBE ACK message, source will resume the data transmission.

(3) No PROBE ACK from D. The source may not receive a reply from destination within a TIMER-EXPIRE for any one of the following reasons: (a) The PROBE packet is dropped by the malicious router and hence D will not return any PROBE ACK to S as it does not know that it was expecting any PROBE packet; (b) The PROBE ACK packet is dropped by the malicious router. To tackle these situations, we propose two requirements. (i) every router buffers the PROBE and PROBE ACK packets. (ii) source router retransmits the PROBE for r attempts because a packet loss can be due to wireless loss or presence of an attacker. After r attempts, if S does not receive a reply from D, it will initiate a hop by hop query for the PROBE and PROBE ACK packets. For e.g, if v_i did not receive the PROBE packet, it implies that node v_{i-1} did not forward the packet and the upstream and downstream neighbors of v_{i-1} can be queried for the opinion and behavior parameters. If misbehaving is detected, source will perform the same operation as listed in case (1).

IV. ESTIMATION OF NORMAL LOSSES

A. Loss due to Wireless Channel

We model the underlying time varying wireless channel as a two-state Markov model [11]. The two state Markov model has two states, g and b, which represents the *good* and *bad* states respectively. When the state is *bad*, all the packets are lost; when the state is *good*, the packets can still be lost due to collision or noise. In the *good* states, losses occur with a probability of P_G while in the *bad* state they happen with a probability of P_B, ($P_G < P_B$). The transition probabilities of the model are defined by P_{bg} between states b and g and P_{gb} between states g and b. The average loss rate, p_e, of the Markov channel is given as $P_G\pi_g + P_B\pi_b$. π_g and π_b are the steady state probabilities and are defined as $\frac{P_{bg}}{P_{bg}+P_{gb}}$ and $\frac{P_{gb}}{P_{bg}+P_{gb}}$ respectively.

Since a wireless mesh network is normally deployed statically for long time, we assume that the channel parameters P_{bg}, P_{gb}, P_G, and P_B can be accurately estimated by observing historical data. Thus, the packet loss probability over the channel p_e can be computed from the channel parameters.

B. Loss due to MAC Layer Collisions

We estimate the probability of collision, p_c, by utilizing the *channel busyness ratio* (CBRO) as discussed in [8]. As opposed to collision probability, CBRO is easy to measure in practice, because IEEE 802.11 is essentially based on virtual and physical carrier sensing methods. During every time period t, each node monitors the wireless medium around it to determine the amount of time the channel is busy, R_b. Once R_b is determined, the node can estimate the probability of collision, p_c, according to the following equations: $R_b = 1 - \frac{p_i\sigma}{p_i\sigma+p_sT_{suc}+p_cT_{col}}$ and $R_s = \frac{p_sT_{suc}}{p_i\sigma+p_sT_{suc}+p_cT_{col}}$. σ is the length of an empty backoff time slot where R_s is the channel utilization ratio. We define T_{suc} and T_{col} respectively as the average time periods associated with successful transmissions and collisions. Further, p_i and p_s denote the probabilities of idle time slot and successful transmission (please refer [8] for the derivation of time periods and probabilities).

In a MAC layer, a lost packet is retransmitted for a certain number of attempts, denoted as γ [8]. However, if all the retransmissions fail, the packet is dropped. Hence, the MAC-layer loss rate due to wireless errors (p_e) and medium access collisions (p_c) are expressed as follows: $L \approx (p_e + p_c)^\gamma$.

V. CONFIGURATION OF OPTIMAL THRESHOLDS

In this section, the optimal thresholds (τ_m^* and τ_l^*) that minimize the sum of false alarm and missed detection probabilities are computed.

A. Probability of False Alarm (P_{FA})

A false alarm occurs when the router gives an alarm but no threats exists. We discuss the following scenarios in which a *normal-behaving* node v_i is reported as suspicious.

False alarm by upstream node, ($P_{FA|A}$). Recall, each upstream node in the forwarding path, e.g., v_{i-1}, overhears downstream's, e.g., v_i's, transmission to determine its behavior. Nonetheless, if an ambiguous collision occurs at v_{i-1} while v_i is forwarding packets to v_{i+1}, node v_{i-1} will fail to overhear v_i's transmission. Hence, v_{i-1} presumes that v_i dropped the packet and increases P_{dt}. For instance, suppose that v_{i-1} successfully forwarded N packets to downstream node v_i. Node v_{i-1} should observe at least $N\tau_m$ misbehaviors to set $O_{v_{i-1}}^{v_i} = 1$. We deduce here that the packet collision happens with an independent probability of p_l (= p_c). Therefore, the false alarm probability ($P_{FA|A}$) is given by:

$$\begin{aligned} P_{FA|A} &= 1 - \sum_{X=0}^{N\tau_m} \binom{N}{X} (p_l^X)(1-p_l)^{(N-X)} \\ &\approx 1 - \frac{1}{\sqrt{2\pi}} \int_{\frac{-Np_l-\frac{1}{2}}{\sqrt{Np_l(1-p_l)}}}^{\frac{N\tau_m - Np_l+1/2}{\sqrt{Np_l(1-p_l)}}} e^{\frac{-y^2}{2}} dy. \end{aligned} \quad (1)$$

where the second step of eqn. (1) is based on the fact that binomial distribution can be well approximated by Gaussian distribution when N is reasonably large [10].

False alarm by downstream node, ($P_{FA|B}$). Recall that the downstream node v_{i+1} observes the loss rate of the link $\{v_i, v_{i+1}\}$ to judge the behavior of upstream node. We deduce here that p_f is the probability with which link $\{v_i, v_{i+1}\}$ experiences higher loss rate than estimated loss (τ_l) due to

ambiguous channel fading. As a result, node v_{i+1} will observe loss rate higher than τ_l and sets $B_{v_{i+1}}^{v_i} = 1$. For e.g., suppose that node v_i forwarded N′ packets to v_{i+1}. Node v_{i+1} should observe at least $Y = N^{'}\tau_l$ misbehaviors to mark v_i as malicious. Therefore, the false alarm probability $(P_{FA|B})$ is given by:

$$P_{FA|B} = 1 - \sum_{Y=0}^{N^{'}\tau_l} \binom{N'}{Y} (p_{lr}^{Y})(1-p_{lr})^{(N'-Y)}$$

$$\approx 1 - \frac{1}{\sqrt{2\pi}} \int_{\frac{-N'p_{lr}-\frac{1}{2}}{\sqrt{N'p_{lr}(1-p_{lr})}}}^{\frac{N'\tau_l - N'p_{lr}+1/2}{\sqrt{N'p_{lr}(1-p_{lr})}}} e^{\frac{-y^2}{2}} dy. \quad (2)$$

where p_{lr} is a function of p_e, p_c and p_f. The false alarm probability $P_{FA|C}$ (for *opinion* and *behavior* parameter =1) is expressed as follows: $P_{FA|C} = P_{FA|A} + P_{FA|B} - P_{FA|A}P_{FA|B}$.

B. Probability of Missed Detection (P_{MD})

A false clear or missed detection probability occurs when the router does not give an alarm and a threat exists. We presume here that node v_i is a gray hole attacker. CAD fails to detect v_i as malicious if the downstream and upstream neighbors of v_i set the detection parameters to zero in the PROBE packet. The missed detection probability, P_{MD}, is given as $P_{MD} = P_{MD|A} \times P_{MD|B}$. $P_{MD|A}$ and $P_{MD|B}$ are the probability that upstream and downstream nodes miss the detection respectively. By exploiting the Gaussian approximation, probabilities are expressed as follows:

$$P_{MD|A} \approx \frac{1}{\sqrt{2\pi}} \int_{\frac{-Np_l'-\frac{1}{2}}{\sqrt{Np_l'(1-p_l')}}}^{\frac{N\tau_m - Np_{l'}+1/2}{\sqrt{Np_{l'}(1-p_{l'})}}} e^{\frac{-y^2}{2}} dy. \quad (3)$$

$$P_{MD|B} \approx \frac{1}{\sqrt{2\pi}} \int_{\frac{-N'p_{lr'}-\frac{1}{2}}{\sqrt{N'p_{lr'}(1-p_{lr'})}}}^{\frac{N'\tau_l - N'p_{lr'}+1/2}{\sqrt{N'p_{lr'}(1-p_{lr'})}}} e^{\frac{-y^2}{2}} dy. \quad (4)$$

$p_{l'}$ is the probability of packets lost due to intentional dropping and ambiguous collisions (p_c) whereas $p_{lr'}$ is the probability of packets lost due to attacker and bad channel quality (p_e, p_c).

We know that while the false alarm probability decreases with an increasing threshold, the missed detection probability in fact increases. It is not difficult to verify that the sum of the false alarm probability and the missed detection probability is a convex function of the thresholds. Thus, an optimal threshold can be derived by minimizing the sum of the false alarm and missed detection probabilities as follows: $\tau_m^* = \min_{\tau_m} [P_{FA|A}(\tau_m) + P_{MD|A}(\tau_m)]$ and $\tau_l^* = \min_{\tau_l} [P_{FA|B}(\tau_l) + P_{MD|B}(\tau_l)]$.

VI. PERFORMANCE EVALUATION

The proposed algorithm is implemented in Ns2 (v2.29) [9] and we study the performance of CAD in terms of: (a) adaption of *thresholds* to varying network load; (b) *routing-related overhead*. The overhead is computed as a ratio of routing-related transmissions to data transmissions [6] where a transmission implies a node either sending or forwarding a packet; and (c) *packet delivery rate* (PDR) of CAD in the "presence" and "absence" of normal losses. Besides comparing the performance of CAD with existing schemes such as BSMR and Watchdog (WD), we also show the performance of CAD with a scenario where "no detection" scheme is employed. The network topology consists of a square grid of 36 mesh routers located in 1000 by 1000 meter area. In our simulations traffic sources are modeled as UDP transfers. Stationary sources and destinations are placed on the opposite sides of the grid with multiple forwarding paths between them. The malicious nodes are randomly located in the forwarding paths of source and destination. We set $r = 2$ for retransmission attempts by source router when a PROBE packet is lost. We modeled the wireless channel as a Markov model and the transition probabilities of this model are expressed as follows: P_{gb}, P_{bg} $=\langle(0,1)(0.3,0.23)(0.4,0.3)(0.45,0.25)(0.45,0.2)\rangle$. For simplicity, we set $P_G = 0$ and $P_B = 1$.

In fig. 1, we study the adaption of the thresholds with the varying network load. We observe that as the load increases, the channel collision probability in fact increases with the channel busyness ratio R_b. Since the thresholds τ_m, τ_l are designed to depend on probability of collisions, we can see an increase in thresholds (τ_m and τ_l) with the increase in probability of collisions. Finally, the graphs also depicts the P_{dt} parameter and the loss rate (L_o) estimated by the upstream and downstream nodes respectively in the presence of 10% dropping by adversaries. Indeed, the misbehaviors observed by the upstream and downstream nodes exceeded the thresholds τ_m and τ_l even in the presence of losses due to collisions and wireless errors. Hence, with CAD we can effectively identify the attackers in the *presence* and *absence* of "natural losses". We also study the impact of PROBE interval (W_s) on the

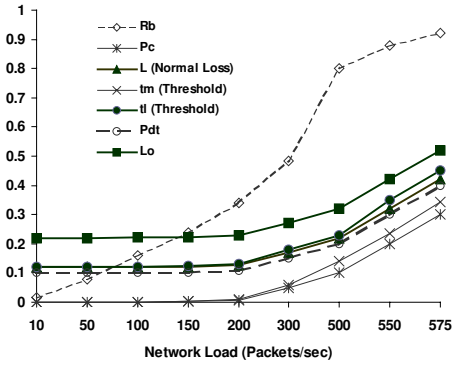

Fig. 1. Adaption of thresholds(τ_m and τ_l) with varying network traffic.The graph also shows the P_{dt} and L_o parameter estimated by the neighbors when attacker launches 10% dropping attack.

performance of CAD. We observe that CAD has high PDR at smaller intervals for e.g., W_s = 10 as opposed to scenarios where PROBE packets are sent at larger intervals for e.g., W_s = 50. The reason for high PDR is that when a PROBE packet is sent within smaller intervals an attacker, if present, will be detected earlier and hence less number of packets will be lost due to malicious behavior. Nevertheless, we also observed that the smaller the interval, CAD has higher routing-

related overhead when compared to larger PROBE intervals. To minimize the packet loss due to attacker(s), we suggest to use smaller packet interval for PROBE. The details are omitted here due to the limited space. In fig. 2 and 3, we study

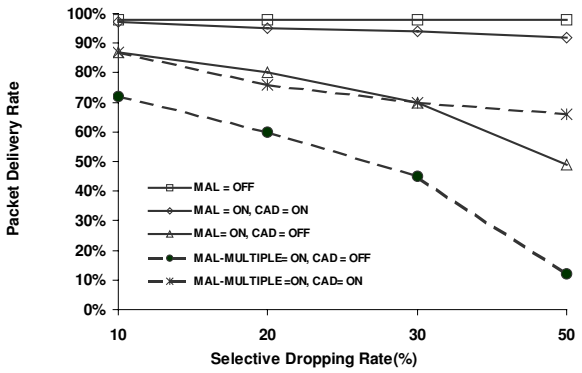

Fig. 2. CAD in the presence of attacker(s). In graphs, the attackers are denoted as "MAL"

how CAD performs in the presence of single and multiple *gray-hole* attackers. In fig. 2, we consider absence of normal losses, while in fig. 3, we assume bad channel quality. It can be inferred from fig. 2 that when "no detection" algorithm is employed, the PDR is degraded in the presence of both *single* (86% in the case of 10% dropping) and *multiple single acting* attackers (73% in the case of 10% dropping). However after using CAD, the PDR is improved to 97% in the case of 10% dropping when single attackers are present and 86% in the case of 10% dropping when multiple attackers are present because CAD detects the attacker and forwards the traffic to the destination through a different path. We also observe that the maximum PDR achieved using the CAD is less than the ideal case, where no routers exhibit malicious behavior (98.1%). The reason behind this is (i) Some packets are already lost before CAD detects the attacker. (ii) After the detection, source queues the packets and will either use another path from route cache or initiate a new route discovery to find an alternate route to avoid the localized router. In fig. 3, we

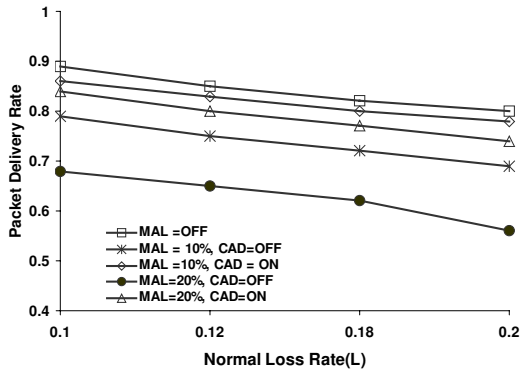

Fig. 3. CAD in the presence of normal losses and attackers. In graphs, the attackers are denoted as "MAL"

study the performance of CAD when packet losses occur due to presence of attacker and normal wireless losses. We observe that the PDR is degraded in the presence of 10% (PDR = 0.79) and 20% (PDR = 0.68) selective dropping attacker respectively when "no detection" algorithm is employed; (c) After using CAD, the PDR is improved to 0.86 in the case of 10% dropping attack and 0.84 in the case of 20% dropping attack. The reason behind this is that unlike prior works, CAD adapts to varying packet losses while setting the detection thresholds τ_l and τ_m. Hence, we can conclude that even in harsh channel conditions, CAD can effectively detect the misbehaving nodes and improve the PDR of the network.

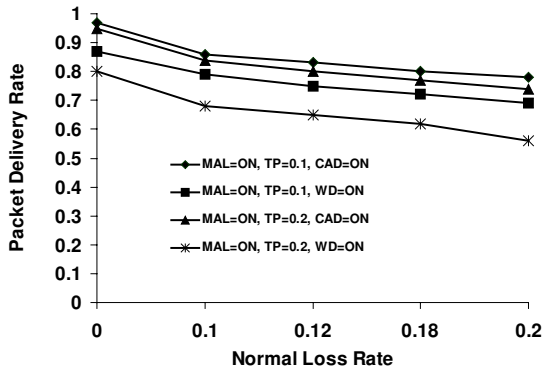

Fig. 4. CAD *vs* Watchdog(WD) in the presence of *limited-transmit power attack* (TP). TP is estimated as the ratio of number of packets lost due to this attack out of number of packets succesfully received by attacker.

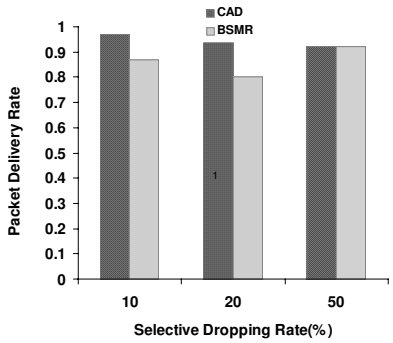

Fig. 5. CAD *vs* BSMR, $\Delta = 2\delta = 20\%$

In fig. 4 and 5, we compare CAD to existing dropping misbehavior detection schemes known as Watchdog (WD) and BSMR. As can be inferred from fig. 4, CAD has better performance (0.97 for TP = 0.1) as opposed to WD (0.87 for TP = 0.1) in the presence of *limited-transmit power* attack because CAD employs both *downstream traffic overhearing* and *upstream hop-by-hop loss observation* to detect the attackers contrary to WD that relies on *downstream traffic monitoring* alone. In fig.5, we observe that PDR of BSMR is degraded in the presence of both 10% and 20% dropping attackers (0.87 for 10% dropping and 0.8 for 20% dropping). The reason behind this is unlike CAD, BSMR employs *static* thresholds that are independent of "natural" losses which inturn prevented BSMR in detecting the 10% and 20% dropping misbehaviors. Hence,

we argue that a channel-aware threshold is *necessary for the accurate detection of attackers*.

VII. Conclusion and Future Work

In this paper, we considered a practical algorithm known as CAD to detect and isolate the selective forwarding attackers in the area of multihop networks such as WMNs. CAD mainly adopts two strategies for detection: *hop-by-hop loss observation by downstream nodes* and *traffic monitoring by upstream nodes*. We also presented a detailed design of the optimal thresholds by analyzing the false alarm and missed detection probabilities of CAD. For future work, we plan to investigate the case that multiple routers may collude with each other.

References

[1] I.F. Akyildiz and X. Wang, "A survey on Wireless Mesh networks," in *IEEE Communications Magazine*, vol. 43, no. 9, pp. S23-S30, Sept. 2005.

[2] E. Cayirci and C. Rong. "Security Attacks in Ad Hoc, Sensor and Mesh Networks," in *Wiley-Interscience*, Jan. 2009.

[3] L. Buttyn and J. Hubaux. "Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing," in *Cambridge University Press*, 2007.

[4] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," in *Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, vol. 1, no. 2-3, pp. 293-315, Sept. 2003.

[5] B. Xiao, B. Yu and C. Gao "CHEMAS: Identify suspect nodes in selective forwarding attacks," in *Journal of Parallel and Distributed Computing*, vol. 67, no. 11, pp. 1218-1230, Nov. 2007.

[6] S. Marti, T. J. Giuli, K. Lai and M. Baker "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. International Conference on Mobile Computing and Networking, MobiCom*, Boston, Massachusetts, 2000.

[7] R. Curtmola, and C. Nita-Rotaru "BSMR: Byzantine-Resilent Secure Multicast Routing in Multi-hop Wireless Networks," in *Proc. of Sensor, Mesh and Ad Hoc Communications and Networks*, Jun. 18-21, 2007.

[8] H. Zhai, X. Chen and Y. Fang "How well can the IEEE 802.11 wireless LAN support quality of service?," in *IEEE Transactions on Wireless Communications*, vol. 4, no.6, pp.3084 - 3094, Nov. 2005.

[9] K. Fall and K. Varadhan, *NS notes and documentation*, The VINT Project, UC Berkely, LBL, USC/ISI, and Xerox PARC, 1997.

[10] H. Stark and J. W. Woods. "Probability and Random Processes With Applications to Signal Processing (3rd edition)," in *Prentice Hall*, July. 2001.

[11] A. Kumar, D. Manjunath and J. Kuri. "Wireless Networking," in *Morgan Kaufmann*, pp. 1-448, 2008.