Routing Misbehavior Detection in MANETs Using an ACK based Scheme

ANNAPURNA VEMPARALA*
Student
Dept of Computer Science Engineering
Bharath University, Chennai, India
anukodali505@gmail.com

Mr.VENKATESAN.K.G
Associate Professor
Dept of Computer Science Engineering
Bharath University, Chennai, India
venkatesh.kgs@gmail.com

Abstract— This paper highlights routing misbehavior in MANETs (Mobile Ad Hoc Networks). In general, routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. However, due to the open structure and scarcely available battery-based energy, node misbehaviors may exist. One such routing misbehavior is that some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets.

In the present studies it is proposed a novel scheme named 2 HOP ACK which provides an add-on technique for routing schemes that detects the routing misbehavior and to overcomes their adverse effect. The main feature of 2 HOP ACK is to send two-hop acknowledgment packets in the opposite direction of the routing path and to reduce additional routing overhead.
The main idea of the 2 HOP ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2 HOP ACK scheme. Analytical and simulation results are presented to evaluate the performance of the proposed scheme.

Introduction

Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes as routers. The operation of MANETs does not depend on preexisting infrastructure or base stations. Network nodes in MANETs are free to move randomly. Therefore, the network topology of a MANET may change rapidly and unpredictably. All network activities, such as discovering the topology and delivering data packets, have to be executed by the nodes themselves, either individually or collectively. Depending on its application, the structure of a MANET may vary from a small, static network that is highly power-constrained to a large-scale, mobile, highly dynamic network.

MANET, all mobile nodes cooperate with each other toward a common goal, such as emergency search/ rescue or military and law enforcement operations. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity. However, some resources are consumed quickly as the nodes participate in the network functions. For instance, battery power is considered to be most important in a mobile environment. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish or misbehaving nodes and their behavior is termed selfishness or misbehavior [2]. One of the major sources of energy consumption in the mobile nodes of MANETs is wireless transmission [3]. A selfish node may refuse to forward data packets for other nodes in order to conserve its own energy.

Several techniques have been proposed to detect and alleviate the effects of such selfish nodes in MANETs. In two techniques were introduced, namely, watchdog and pathrater, to detect and mitigate the effects of the routing misbehavior, respectively. The watch-dog technique identifies the misbehaving nodes by over-hearing on the wireless medium. The pathrater technique allows nodes to avoid the use of the misbehaving nodes in any future route selections. The watchdog technique is based on passive overhearing. Unfortunately, it can only determine whether or not the next-hop node sends out the data packet. The reception status of the next-hop link's receiver is usually unknown to the observer.Misbehavior Detection and Mitigation

. In MANETs, routing misbehavior can severely degrade the performance at the routing layer. Specifically, nodes may participate in the route discovery and maintenance processes but refuse to forward data packets. How do we detect such misbehavior? How can we make such detection processes more efficient (i.e., with less control overhead) and accurate (i.e., with low false alarm rate and missed detection rate.

successfully over the next hop, the destination node of the next-hop link will send back a special two-hop acknowl-edgment called 2 HOP ACK to indicate that the data packet has been received successfully. Such a 2 HOP ACK transmission takes place for only a fraction of data packets, but not all. Such a "selective" acknowledgment[1] is intended to reduce the additional routing overhead caused by the 2 HOP ACK scheme. Judgment on node behavior is made after observing its behavior for a certain period of time

2 Related Work

The security problem and the misbehavior problem of wireless networks including MANETs have been studied by many researchers, Various techniques have been proposed to prevent selfishness in MANETs. These schemes can be broadly classified into two categories: credit-based schemes and reputation-based schemes.

2.1 Misbehaving Routes

In order to demonstrate the adverse effect of routing misbehavior, it is proposed to estimate the probability of misbehaving routes. A route which misbehaves when there is at least one router along the same route is termed as misbehaving route. The analysis was carried out with the following assumptions.

The network nodes are randomly distributed over the entire network area. Each node's location are independent of other. There are N nodes in the network area of size X ∗ Y ; The source and the destination of each transmissions were chosen randomly among other nodes; · Nodes (other than the source and thedestination) are chosen as misbehaving nodesand are independent with probability denoted as pm. The routes are examined with an average number of hops, h. There are h−1 routers between the source and the destination. Each of these routers may misbehave with that of probability (pm).

The main problem with credit-based schemes is that they usually require some kind of tamper-resistant hardware and/or extra protection for the virtual currency or the payment system. We focus on reputation-based techniques in this paper instead.

2.2 Reputation-Based Schemes

The second category of techniques to combat node misbehavior in MANETs is reputation-based [4], [7]. In such schemes, network nodes collectively detect and declare the misbehavior of a suspicious node. Such a declaration is then propagated throughout the network so that the misbehav-ing node will be cut off from the rest of the network.

In [4], Marti et al. proposed a scheme that contains two major modules, termed watchdog and pathrater, to detect and mitigate, respectively, routing misbehavior in MANETs. Nodes operate in a promiscuous mode wherein the watch-dog module overhears the medium to check whether the next-hop node faithfully forwards the packet. At the same time, it maintains a buffer of recently sent packets. A data packet is cleared from the buffer when the watchdog overhears the same packet being forwarded by the next-hop node over the medium. If a data packet remains in the buffer for too long, the watchdog module accuses the next-hop neighbor of misbehaving. Thus, the watchdog enables misbehavior detection at the forwarding level as well as the link level. Based on the watchdog's accusations, the pathrater module rates every path in its cache and subsequently chooses the path that best avoids misbehaving nodes. Due to its reliance on overhearing, however, the watchdog technique may fail to detect misbehavior or raise false alarms in the presence of ambiguous collisions, receiver collisions, and limited transmission power, as explained in [4].

The CONFIDANT protocol proposed by Buchegger and Le Boudec in [7] is another example of reputation-based schemes. The protocol is based on selective altruism and utilitarianism, thus making misbehavior unattractive. CON-FIDANT consists of four important components—the Monitor, the Reputation System, the Path Manager, and the Trust Manager. They perform the vital functions of neighborhood watching, node rating, path rating, and sending and receiving alarm messages, respectively. Each node continuously monitors the behavior of its first-hop neighbors. If a suspicious event is detected details of the event are passed to the Reputation System. Depending on how significant and how frequent the event is, the

Reputation System modifies the rating of the suspected node. Once the rating of a node becomes intolerable, control is passed to the Path Manager, which accordingly controls the route cache. Warning messages are propagated to other nodes in the form of an Alarm message sent out by the Trust Manager.

The Monitor component in the CONFIDANT scheme observes the next hop neighbor's behavior using the overhearing technique. This causes the scheme to suffer from the same problems as the watchdog scheme.

In Miranda and Rodrigues adopted a similar approach. Each node i maintains a data structure Status$_i$½j& about every other node j as an indication of what impression node i has about node j. Along with a credit counter, node i also maintains lists of nodes to which node j will and will not provide service. Every node periodically broadcasts relevant information in the form of a self-state message. Other nodes update their own lists based on the information contained in these self-state messages.

2.3 End-to-End Acknowledgment Schemes

There are several schemes that use end-to-end acknow-ledgments (ACKs) to detect routing misbehavior or malicious nodes in wireless networks.

In the TCP protocol, end-to-end acknowledgment is employed. Such acknowledgments are sent by the end-receiver to notify the sender about the reception of data packets up to some locations of the continuous data stream. The Selective Acknowledgment (SACK) technique is used to acknowledge out-of-order data blocks.

The 2 HOP ACK technique differs from the ACK and the SACK schemes in the TCP protocol in the following manner: The 2 HOP ACK scheme tries to detect those misbehav-ing nodes which have agreed to forward data packets for the source node but refuse to do so when data packets arrive. TCP, on the other hand, uses ACK and SACK to measure the usefulness of the current route and to take appropriate action. For example, congestion control is based on the reception of the ACK and the SACK packets.

In order to identify malicious routers that draw traffic toward themselves but fail to correctly forward the traffic, Padmanabhan and Simon proposed the secure traceroute protocol [16]. The normal traceroute protocol allows the sender to simply send packets with increasing Time-To-Live (TTL) values and wait for a warning message from the router at which time the packet's TTL value expires. The secure traceroute protocol authenticates the traceroute packets and disguises them as regular data packets.

The Best-effort Fault-Tolerant Routing (BFTR) scheme due to

Xue and Nahrstedt [18] also employs end-to-end ACKs. The BFTR scheme continuously monitors the quality (i.e., packet delivery ratio) of the path in use. This is compared with the predefined expected behavior of good routes. If the behavior of the route in use deviates from the behavior of good routes, it is marked as "infeasible" and a new route is used. Since BFTR throws out the entire route before detecting the misbehaving nodes, the newly chosen route may still include the same misbehaving nodes. Even though the new route will be detected as infeasible by the source after a period of observation time, data packet loss will occur in traffic flows when using protocols such as UDP. Such a repeated detection process is inefficient.

2.4 Other Prior State-of-the-Art Schemes

The misbehavior problem that we focus on in this work was referred to as the Black Hole attack in Aad et al. investigated the JellyFish attack for closed-loop flows such as TCP. It was shown that a JellyFish attacker may stealthily rearrange, delay, or periodically drop packets while still remaining protocol-compliant. Such attacks may cause end-to-end throughput of closed-loop flows to drop. Similarly, the Black Hole attack was also shown to have adverse effect on open-loop flows such as UDP. Unlike [14], we propose a 2 HOP ACK technique to detect such misbehaviors.

2.5 The TWOACK and S-TWOACK Schemes

In we proposed an early version of the 2 HOP ACK scheme, termed TWOACK. The 2 HOP ACK and the TWOACK schemes have the following major differences: 1) The receiving node in the 2 HOP ACK scheme only sends 2 HOP ACK packets for a fraction of received data packets, while, in the TWOACK scheme, TWOACK packets are sent for every data packet received. Acknowledging a fraction of received data packets gives the 2 HOP ACK scheme better performance with respect to routing overhead. 2) The 2 HOP ACK scheme has an authentication mechanism to make sure that the 2 HOP ACK packets are genuine.

The Selective TWOACK (S-TWOACK) scheme proposed in is different from 2 HOP ACK as well. Mainly, each TWOACK packet in the S-TWOACK scheme acknowledges the receipt of a number of data packets, but a 2 HOP ACK packet in the 2 HOP ACK scheme only acknowledges one data packet. With such a subtle change, the 2 HOP ACK scheme has easier control over the trade-off between the performance of the network and the cost as compared to the S-TWOACK scheme.

3 PROBLEM OF ROUTING MISBEHAVIOR

In this section, we describe the problems caused by routing misbehavior. But first, we summarize the notations and assumptions used throughout this paper.

3.1 Routing Misbehavior Model

We present the routing misbehavior model considered in this paper in the context of the DSR protocol.Due to DSR's popularity, we use it as the basic routing protocol to illustrate our proposed add-on scheme. The details of DSR can be found in the implementation of our scheme as an add-on to other routing schemes

We focus on the following routing misbehavior: A selfish node does not perform the packet forwarding function for data packets unrelated to itself.[2] However, it operates normally in the Route Discovery and the Route Mainte-nance phases of the DSR protocol. Since such misbehaving nodes participate in the Route Discovery phase, they may be included in the routes chosen to forward the data packets from the source. The misbehaving nodes, however, refuse to forward the data packets from the source. This leads to the source being confused.

In guaranteed services such as TCP, the source node may either choose an alternate route from its route cache or initiate a new Route Discovery process. The alternate route may again contain misbehaving nodes and, therefore, the data transmission may fail again. The new Route Discovery phase will return a similar set of routes, including the misbehaving nodes. Eventually, the source node may conclude that routes are unavailable to deliver the data packets. As a result, the network fails to provide reliable communication for the source node even though such routes are available. In best-effort services such as UDP, the source simply sends out data packets to the next-hop node, which forwards them on. The existence of a misbehaving node on the route will cut off the data traffic flow. The source has no knowledge of this at all.

In this paper, we propose the 2 HOP ACK technique to detect such misbehaving nodes. Routes containing such nodes will be eliminated from consideration. The source node will be able to choose an appropriate route to send its data. In this work, we use both UDP and TCP to demonstrate the adverse effect of routing misbehavior and the performance of our proposed scheme.

The attackers (misbehaving nodes) are assumed to be capable of performing the following tasks:

. dropping any data packet,
. masquerading as the node that is the receiver of its next link,
. sending out fabricated 2 HOP ACK packets,
. sending out fabricated h_n, the key generated by the 2 HOP ACK packet senders, and
. claiming falsely that its neighbor or next-hop links are misbehaving.

3.2 Probability of Misbehaving Routes

We have compared the numerical results based on (6) and simulation results. Our simulation results were obtained through 20 runs with different seeds in NS2. In Table 1, we show the results for different network areas and number of nodes. The transmission range is R ¼ 250 m for every node.

TABLE 1
Probability of Misbehaving Routes
for Different Misbehavior Ratio, p_m

Results for $p_m = 0.1$			
Network Area, X*Y	4R*4R	5R*5R	10R*10R
Number of Nodes, N	70	100	400
Analytical Results	0.18	0.25	0.49
Simulation Results	0.17	0.22	0.43

4 THE 2 HOP ACK SCHEME

The watchdog detection mechanism in has a very low overhead. Unfortunately, the watchdog technique suffers from several problems such as ambiguous collisions, receiver collisions, and limited transmission power. The main issue is that the event of successful packet reception can only be accurately determined at the receiver of the next-hop link, but the watchdog technique only monitors the transmission from the sender of the next-hop link.

Noting that a misbehaving node can either be the sender or the receiver of the next-hop link, we focus on the problem of detecting misbehaving links instead of misbehaving nodes.

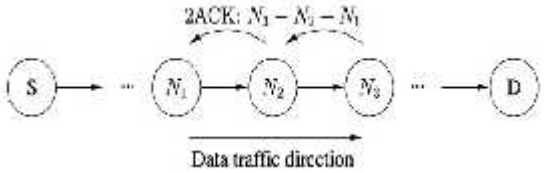

Fig. 1: The 2 HOP ACK scheme

In the next-hop link, a misbehaving sender or a misbehav-ing receiver has a similar adverse effect on the data packet: It will not be forwarded further. The result is that this link will be tagged [17]. Our approach discussed here signifi-cantly simplifies the detection mechanism.

4.1 Details of the 2 HOP ACK Scheme

The 2 HOP ACK scheme is a network-layer technique to detect misbehaving links and to mitigate their effects. It can be implemented as an add-on to existing routing protocols for MANETs, such as DSR. The 2 HOP ACK scheme detects misbehavior through the use of a new type of acknowl-edgment packet, termed 2 HOP ACK. A 2 HOP ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route.

Fig. 1 illustrates the operation of the 2 HOP ACK scheme. Suppose that N_1, N_2, and N_3 are three consecutive nodes (triplet) along a route. The route from a source node, S, to a destination node, D, is generated in the Route Discovery phase of the DSR protocol. When N_1 sends a data packet to N_2 and N_2 forwards it to N_3, it is unclear to N_1 whether N_3 receives the data packet successfully or not. Such an ambiguity exists even when there are no misbehaving nodes. The problem becomes much more severe in open MANETs with potential misbehaving nodes.

The 2 HOP ACK scheme requires an explicit acknowledgment to be sent by N_3 to notify N_1 of its successful reception of a data packet: When node N_3 receives the data packet successfully, it sends out a 2 HOP ACK packet over two hops to N_1 (i.e., the opposite direction of the routing path as shown), with the ID of the corresponding data packet. The triplet $½N_1$! N_2 ! N_3& is derived from the route of the original data traffic. Such a triplet is used by N_1 to monitor the link N_2 ! N_3. For convenience of presentation, we term N_1 in the triplet $½N_1$! N_2 ! N_3& the 2 HOP ACK packet receiver or the observing node and N_3 the 2 HOP ACK packet sender.

Such a 2 HOP ACK transmission takes place for every set of triplets along the route. Therefore, only the first router from the source will not serve as a 2 HOP ACK packet sender. The last router just before the destination and the destination will not serve as 2 HOP ACK receivers.[4]

To detect misbehavior, the 2 HOP ACK packet sender main-tains a list of IDs of data packets that have been sent out but have not been acknowledged. For example, after N_1 sends a data packet on a particular path, say, $½N_1$! N_2 !

The 2 HOP ACK packet is different from the selective acknowledgment (SACK) [24] in TCP. The SACK packets are used by the TCP data receiver to acknowledge noncontiguous blocks of data that are not covered by the Cumulative Acknowledgment field. A 2 HOP ACK packet, on the other hand, acknowledges the received data packet. In addition, the SACK packets are sent by the data traffic receiver, but the 2 HOP ACK packets are sent by the third node in every set of triplets along the traffic route.2 HOP ACK technique solves this problem by requiring N3 to send a 2 HOP ACK packet explicitly Receiver Collisions.

A counter of forwarded data packets, C , is incremented 2 HOP ACK packets. pkts simultaneously. . Limited Transmission Power. A misbehaving N 2 At N , each ID will stay on the list for seconds, the may maneuver its transmission power such that N timeout for 2 HOP ACK reception. If a 2 HOP ACK packet correspond- can overhear its transmission but N cannot. This ing to this ID arrives before the timer expires, the ID will be problem is similar to the Receiver Collisions pro- removed from the list. Otherwise, the ID will be removed at blem. It becomes a threat only when the distance the end of its timeout interval and a counter called C will between N and N is less than that between N and m is be incremented.The 2 HOP ACK scheme is immune to limited When N receives a data packet, it determines whether it transmission power problem.needs to send a 2 HOP ACK packet to N.

In order to reduce the Limited Overhearing Range. A well-behaved additional routing overhead caused by the 2 HOP ACK scheme, may use low transmission power to send data only a fraction of the data packets will be acknowledged via toward N . Due to N 's limited overhearing range, 2 HOP ACK packets. Such a fraction is termed the acknowl- it will not overhear the transmission successfully edgment ratio, R . By varying R , we can dynamically and will thus infer that N is misbehaving, causing ack tune the overhead of 2 HOP ACK packet transmissions. false alarm.

Both this problem and the limited Node Nobserves the behavior of link N ! N for a transmission power problem are caused by the period of time termed T. At the end of the observation potential asymmetry of communication links. The ob s period, N calculates

the ratio of missing 2 HOP ACK packets as 2 HOP ACK scheme is immune to the limited overhearing C=C and compares it with a threshold R . If the ratio range issue. m is pkts m is is greater than R , link N ! N is declared misbehaving With the explicit requirement of 2 HOP ACK transmissions, and N sends out an RERR (or the misbehavior report) the 2 HOP ACK scheme solves the above problems. Compared packet. The data structure of RERR is shown in Fig. 3. Since with overhearing techniques, the 2 HOP ACK scheme has a only a fraction of the received data packets are acknowledge disadvantage of higher routing overhead. This additional edged, R should satisfy R in order to ack routing overhead is caused by the transmission of 2 HOP ACK eliminate false alarms caused by such a partial acknowledgement packets.

The output has a fixed length. interested in forging a new h. Since a majority of the n . HðxÞ is relatively easy to compute for any given nodes are well-behaved, the true value of h can be N input x. obtained. . It is computationally infeasible to calculate x from Once the h element is distributed from N to N , N can n 3 1 3 HðxÞ. use h (0< i<n) sequentially to sign the 2 HOP ACK packets to
. HðxÞ is collision-free. I be sent to N . The h elements will be disclosed by N one at i.

The collision-free property assures that the hash results a time. are unique. Examples of such hash functions include MD5 Assume that h has been disclosed (initially, i ¼ n 1). and SHA1. When node N needs to send a 2 HOP ACK packet, it calculates a To create a one-way hash chain, a node picks up a Message Authentication Code (MAC) based on h , i 1 random initial value x 2f0; 1g and computes its hash ½N ;N ;ID , and attaches the MAC and the h
value to I ,h value. The first number in the hash chain h is initialized to i 1 the 2 HOP ACK packet. Fig. 4 illustrates the packet format of a 0 x. By using the general formula h ¼ Hðh Þ, for 0 <i n, 2 HOP ACK packet. The fields in Fig. 4 are explained below: I i 1 for some n, a chain of h is formed: I . N : the receiver of the next hop, in the opposite 2 h

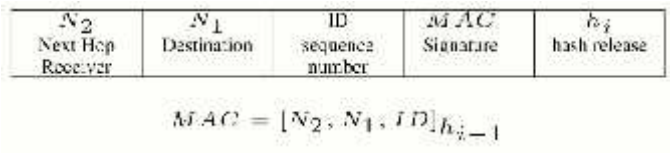

Fig. 2. The packet format of 2 HOP ACK. implemented relying on asymmetric cryptography, using N .

This technique bypasses N , the potential threat to the techniques such as RSA . However, such asymmetric distribution of h.While such a technique consumes more n operations are too expensive for the mobile nodes in energy from node N , it takes place rather infrequently. It MANETs which are usually resource constrained. will be seen later that every 2 HOP ACK packet uses one In [26], an efficient algorithm termed one-way hash chain element in the one-way hash chain in (7). The distribution [27] was used to guard against security attacks such as DoS of a new h element is only needed when the entire chain n and resource consumption attacks in the destination- has been used. sequenced distance vector (DSDV) routing protocol [28]. A An alternative technique to delivering the h element is n one-way hash chain can be constructed based on a one-way the “multipath transmission” mechanism. In this method, hash function, H . The hash function is a transformation that N sends its h through a number of different paths. For n takes a variable-length input and returns a fixed-length bit instance, a packet carrying the h element may be flooded.

An ideal hash (TTL) value of two or three hops. This is similar to the function H should have the following properties: broadcast of the RREQ packets in DSR. N employs a majority vote technique to obtain h after it receives several n . The input can be of any length. copies of h . Note that only the misbehaving N is n 2 . The output has a fixed length. interested in forging a new h . Since a majority of the n . HðxÞ is relatively easy to compute for any given nodes are well-behaved, the true value of h can be n input x. obtained. . It is computationally infeasible to calculate x from Once the h element is distributed from N to N. use h (0 i<n) sequentially to sign the 2 HOP ACK packets to . HðxÞ is collision-free. I be sent to N . The h elements will be disclosed by N one at 1 I 3 The collision-free property assures that the hash results a time. are unique. Examples of such hash functions include MD5 Assume that h has been disclosed (initially, i ¼ n 1). iþ 1 and SHA1 . When node N needs to send a 2 HOP ACK packet, it calculates a 3 To create a one-way hash chain, a node picks up a Message Authentication Code (MAC) based on h , i 1 random initial value x 2f0; 1g and computes its hash ½N ;N ;ID , and attaches the MAC and the h value to I h value. The first number in the hash chain h is initialized to i 1 the 2 HOP ACK packet. Fig. 4 illustrates the packet format of a 0 x. By using the general formula h ¼ Hðh Þ, for 0 <i n, 2 HOP ACK packet. The fields in Fig. 4 are explained below: I i 1 for some n, a chain of h is formed: I . N : the receiver of the next hop, in the opposite direction of the route.The destination of the 2 HOP ACK packet, the obser- It can be proven that, given an existing authenticated gving node, that is two-hop away from the 2 HOP ACK element of a one-way hash chain, it is feasible to verify the
packet sender. other elements preceding it. For example, given an . ID: the sequence number of the corresponding data authenticated value of h , a node can authenticate h n n 3 packet.

5. PERFORMANC EVALUATION

May slow down or even stop sending packets. Therefore, a In this section, we present our simulation results for more reasonable performance metric is the total number of performance evaluation. Since the 2 HOP ACK scheme works as packets that are received at the destination. We compared a an add-on technique for the DSR protocol, the performance relative throughput, a normalized number of packets that of the 2 HOP ACK scheme is actually the performance of the are received, of different schemes in the TCP traffic scenario. DSR+2 HOP ACK

scheme.

5.1 Simulation Methodology and Performance

The packet delivery ratio of the 2 HOP ACK Metrics scheme, the BFTR scheme, the S-TWOACK scheme, In the simulations, we used a version of Network Simulator and the original DSR protocol as a function of misbehavior (ns-2) that includes wireless extensions developed by ratio, p. We varied p from 0 (all of the nodes are well- m m the CMU Monarch project group. We modified the DSR behaved) to 0.4 (40 percent of the nodes misbehave). The module in ns-2 to simulate misbehaving nodes.

The maximum speed is V ¼ 20 m/sec. From the figure, we can m observation period of the 2 HOP ACK scheme was set to T ¼ observe that most packets were delivered by all four ob s 0:8 second. Unless specified otherwise, the 2 HOP ACK scheme schemes when p ¼ 0 (no misbehaving nodes). The packet m used R ¼ 0:20, R ¼ 0:85, and a timeout value of ¼ delivery ratio decreases as p
increases. For example, given an . ID: the sequence number of the corresponding data authenticated value of h , a node can authenticate h n n 3 packet. For n takes a variable-length input and returns a fixed-length bit instance, a packet carrying the h element may be flooded.

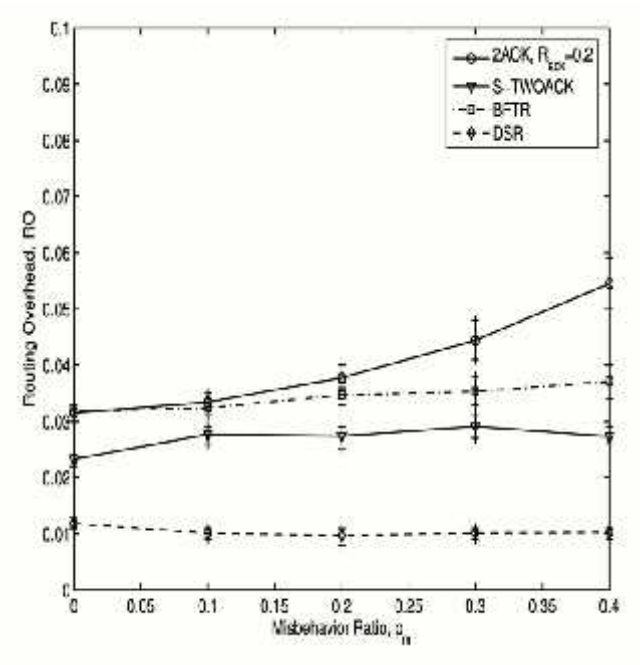

Fig 3: Packet Delivery ratio of 2 ACK ,BFTR, S-TWOACK DSR

Compared with the ack m is m 0:15 second. original DSR scheme, the 2 HOP ACK scheme maintains a much The IEEE 802.11 MAC was used with a channel data rate higher PDR. For example, the 2 HOP ACK scheme delivered over of 11 Mbps. The data packet size was 512 bytes. The 90 percent of data packets even when p ¼ 0:4. The rest of m wireless transmission range of each node was R ¼ 250 m. In the packets were dropped because no well-behaved routes the simulations, N ¼ 50 mobile nodes were randomly could be found from the source to the destination. On the distributed in a 700 m by 700 m flat area. The source and other hand, DSR delivered about 40 percent of the packetsin the same scenario.

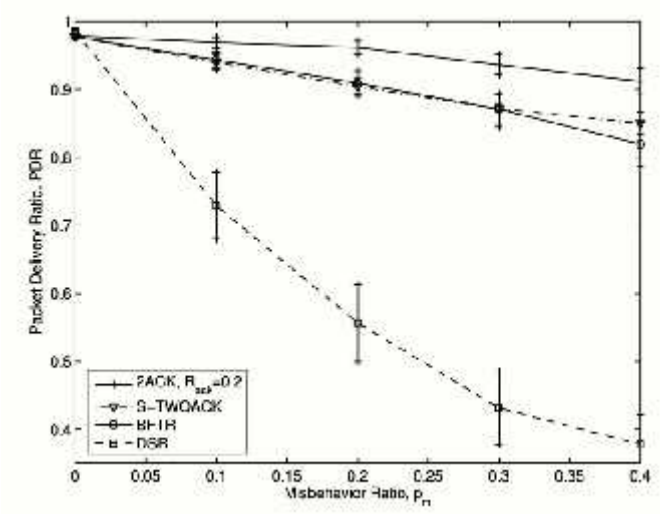

Fig 4:: Routing Overhead of 2 ACK ,BFTR, S-TWOACK DSR

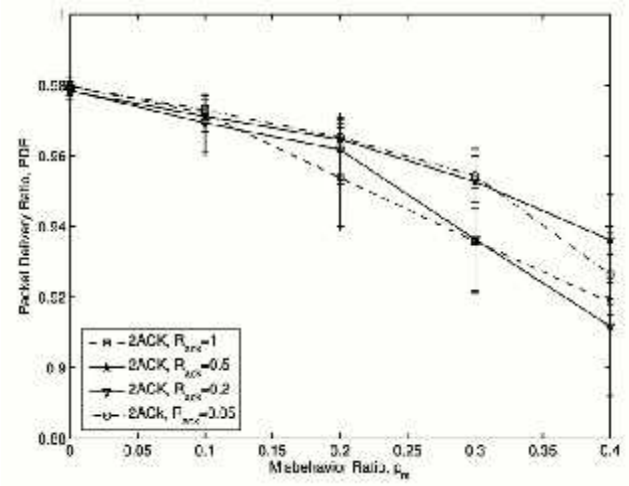

Fig 5: Packet delivery ratio of 2 ACK for different R

to report misbehaviors and to find alternate routes in a more TWO ACK packetis sentfor every five consecutively received hostile network environment. data packets [23], have similar PDR

performance. Both are In Fig. 7, we show the PDR of the 2 HOP ACK scheme with outperformed by the 2 HOP ACK scheme. For example, the BFTR different acknowledgment ratios, R . The acknowledg- scheme delivered roughly 82 percent and the S-TWOACK ack ment ratio R was set to 0.05, 0.2, 0.50, and 1.0, scheme delivered about 85 percent data packets when ack respectively. The corresponding R was 0.98, 0.85, 0.6, p ¼ 0:4. Compared with the 2 HOP ACK scheme, since the BFTR mi s m and 0.33, respectively. Note that R and R need to scheme does not detect a misbehaving node/link, it may m i s ack satisfy (8). Based on Fig. 5, we can see that the PDR choose an alternate route which still contains the misbehav- performance of the 2 HOP ACK scheme is not appreciablying node. The S-TWOACK scheme takes more time to detect affected by R misbehaving links, causing more packets being dropped a c k We compare the routing overhead of the 2 HOP ACK scheme before an alternate route is used.

With different R values in Fig. 4. As expected, the routing In Fig. 6, we compare the routing overhead of the 2 HOP ACK ack overhead of the 2 HOP ACK scheme is the highest when R ¼ 1. scheme (with R ¼ 0:2), the BFTR scheme, the S-TWOACK ack This is due to the large number of 2 HOP ACK packets scheme (with maximum_IDs_Carried = 5), and the DSR transmitted in the network. As the value of R decreases, scheme. The higher routing overhead in the 2 HOP ACK and the ack the routing overhead reduces dramatically. Therefore, R S-TWOACK schemes is due to the transmission of extra The extra routing overhead of the routing overhead. BFTR scheme is caused by the extra route discovery Comparing Fig. 8 and Fig. 6, we have the following processes. The overhead of 2 HOP ACK increases with the observations on routing overhead:

As R decreases, the increase of misbehavior percentage. This is because more ac k routing overhead of the 2 HOP ACK scheme reduces to a level RERR (the misbehavior report) and RREQ packets are sent Fig. 6. Routing overhead of 2 HOP ACK with different R ack.

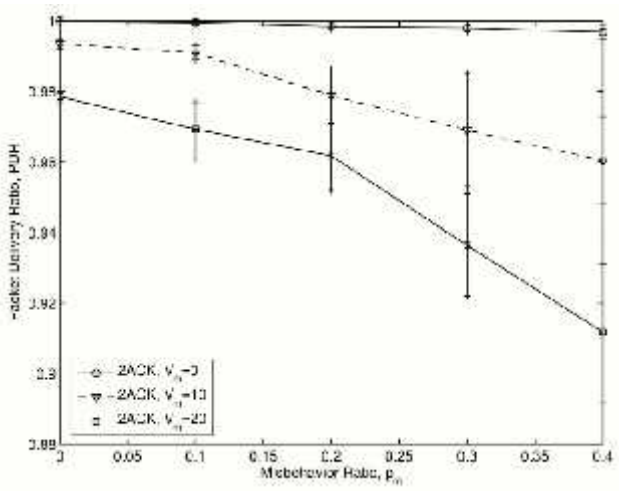

Fig 6: The Packet delivery ratio of 2 ACK for different V

than that of the DSR scheme at p ¼ 0. This is due to the The 2 HOP ACK scheme has been implemented on top of DSR. M false alarm reports in the 2 HOP ACK scheme in a high mobility It is also possible to implement the 2 HOP ACK scheme over other network.

6. CONCLUSIONS AND FUTURE WORK

The main challenge is how to derive the Note that comparisons cannot be made directly between triplet information so that the 2 HOP ACK sender and the the values in Fig. 5 and the numbers in Table 2. The former observing node are informed of such information. Knowledge of topology of the 2-hop neighborhood may be used. represents packet delivery ratio (PDR); the latter represents In addition, the 2 HOP ACK scheme can only work in managed the total number of packets that are received (normalized MANETs (as compared to open MANETs). The main over a fixed number, the average number of packets reason is that parameters such as R and R need to transmitted). Ack m is be set. In our future work, we will investigate how to add the 2 HOP ACK scheme to other types of routing schemes. open networks. Theoretical analysis of the performance Mobile Ad Hoc Networks (MANETs) have been an area for gain of the 2 HOP ACK scheme is of interest as well. active research over the past few years due to their potentially widespread application in military and civilian DSR in MANETs.

ACKNOWLEDGMENTS

[1] K. Balakrishnan, J. Deng, and P.K. Varshney, “TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks,” Proc. IEEE This work was supported in part by the SUPRIA program Wireless Comm. and Networking Conf. (WCNC ’05), Mar. 2005. of the CASE Center at Syracuse University and Louisiana

[2] M. Mathis, J. Mahdavi, S. Floyd, and A. Romanow, “RFC 2018—TCP Selective Acknowledgement Options,” technical re- EPSCoR Pfund LBOR0049PR00C. The authors would like to port, PSC, LBNL, Sun Microsystems, Oct. 1996.

thank the associate editor, Dr. J.-P. Hubaux, and the three

[3] D.B. Johnson, "ECC, Future Resiliency and High Security anonymous reviewers for their valuable comments to Systems,"white paper, Certicom, www.certicom.com, Mar. 1999.
[4] Y. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient improve this paper. The authors thank Y. Xue and Distance Vector Routing for Mobile Wireless Ad Hoc Networks," K. Nahrstedt for providing the simulation code for the Ad Hoc Networks, vol. 1, no. 1, pp. 175-192, 2003. BFTR scheme [18].
[5] L. Lamport, "Password Authentication with Insecure Communication," Comm. ACM, vol. 24, no. 11, pp. 770-772, Nov. 1981.
[6] C.E. Perkins and P. Bhagwat, "Highly Dynamic Destination-R Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Proc. ACM Special Interest Group on Data Comm. (SIGCOMM [1] H. Miranda and L. Rodrigues, "Preventing Selfishness in Open '94), pp. 234-244, Aug. 1994. Mobile Ad Hoc Networks," Proc. Seventh CaberNet Radicals
[7] R.L. Rivest, "RFC 1321—The MD5 Message-Digest Algorithm," Workshop, Oct. 2002. technical report, MIT Laboratory for Computer Science and RSa
[8] L. Buttyan and J.-P. Hubaux, "Security and Cooperation in Data Security, Inc., Apr. 1992.
Wireless Networks," http://secowinet.epfl.ch/, 2006.
[9] D. Eastlake and P. Jones, "RFC 3174—US Secure Hash Algorithm
[10] L.M. Feeney and M. Nilsson, "Investigating the Energy Con-1 (SHA1)," technical report, Motorola and Cisco Systems, Sept. sumption of a Wireless Network Interface in an Ad Hoc 2001. Networking Environment," Proc. IEEE INFOCOM, 2001.
[11] "The Network Simulator (ns-2)," http://www.isi.edu/nsnam/
[12] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing ns/, 2005. Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom, Aug.
[13] J.Y. Le Boudec and M. Vojnovic, "Perfect Simulation and 2000. Stationarity of a Class of Mobility Models," Proc. INFOCOM,
[14] L. Buttyan and J.-P. Hubaux, "Enforcing Service Availability in Mar. 2005. Mobile Ad-Hoc WANs," Proc. MobiHoc, Aug. 2000.
[15] J.-P. Hubaux, T. Gross, J.-Y. LeBoudec, and M. Vetterli, "Toward Self-Organized Mobile Ad Hoc Networks: The Terminodes Project," IEEE Comm. Magazine, Jan. 2001.
[16] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks," Proc. MobiHoc, June 2002.
[17] S. Zhong, J. Chen, and Y.R. Yang, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks," Proc. INFOCOM, Mar.-Apr. 2003.