The Case for End-to-End Solutions to Secure Routing in MANETs

Stephen Dabideen*
*Department of Computer Engineering
University of California, Santa Cruz
Santa Cruz, CA 95064
Email: dabideen@soe.ucsc.edu

Bradley R. Smith*
† Department of Computer Engineering
University of California, Santa Cruz
Santa Cruz, CA 95064
Email: brad@soe.ucsc.edu

J.J. Garcia-Luna-Aceves†*
† Palo Alto Research Center
3333 Coyote Hill Road
Palo Alto, CA 94304
Email: jj@soe.ucsc.edu

***Abstract*—Providing secure routing in MANETs is far more difficult than in wired networks or static wireless networks. Node mobility and the relative scarcity of bandwidth render prior solutions ineffective. Solutions based on securing link or path information do not work well in MANETs because the dynamic nature of links requires extensive use of flooding. On the other hand, solutions based on hop-by-hop exchanges of distance information are easily compromised. Furthermore, path discovery does not necessarily translate into data delivery. We argue that secure routing in MANETs must be based on the end-to-end verification of physical-path characteristics aided by the exploitation of path diversity to find secure paths. We apply this approach to the design of the Secure Routing through Diversity and Verification (SRDV) protocol, a secure routing protocol that we show to be as efficient as unsecure on-demand or proactive routing approaches in the absence of attacks.**

I. Introduction

A secured routing protocol, in the most general sense, must deliver uncorrupted data packets to the destination. To achieve this, it is necessary to secure both the control plane (ensuring path discovery) and the data plane of the protocol.

Much of the research in this area has been devoted to securing the control plane and rely on securing entire paths or having each node along the path secure the link it intends to use (e.g., [3], [2]). However, this is not a viable approach for large MANETs because it leads to unsustainable flooding of control packets. On the other hand, hop-by-hop approaches, that rely on nodes updating and advertising their distances, are difficult to secure because adversaries can misrepresent their distances to destinations without detection. Section II presents a summary of prior approaches for secure routing in MANETs.

Many attacks are aimed at forcing data to be routed through adversary nodes, and once this is done they can perform denial of service, or disclosure attacks. It is possible that data can be routed, without any manipulation of the network, through adversaries and securing only the control plane would provide no defense. Such attacks can be best detected, and arguably can *only* be detected by end-to-end means. If these attacks were to occur when the known topology information is correct, then the best means of defense is path diversity. Previous work towards securing the data plane has employed feedback and path diversity [10], but these rely on assigning weights to each explicitly recorded path, thus requiring complete path information, and most often source routing. In a MANET, paths are transient and assigning a weight to a path is of little value since, by the time the appropriate weight is determined, the path may no longer exist. Instead of assigning a weight to a precisely defined path, we argue that the weights should to assigned to families of paths thus extending the usefulness of information. Also, incremental routing (as opposed to source routing) is more flexible and can lead to better performance. We take the security one step further and use physical path characteristics such as measured delay and bandwidth to preemptively avoid suspicious paths.

We introduce the *Secure Routing through Diversity and Verification* protocol (SRDV) in Section III. The goal of SRDV is to efficiently compute and use the shortest un-compromised paths available for the transmission of data through a network. SRDV accomplishes this by computing paths on-demand to minimize routing overhead, ensuring the correctness and freshness of signaling through the use of digital signatures, sequence numbers, and hash chain authentication, *verifying* the performance of these paths with end-to-end probing to detect compromised paths, and load-balancing over a *diverse* set of paths (the region of interest) to counter attacks once detected. SRDV accomplishes this while using comparable, if not less, overhead than many traditional unsecured approaches.

Section IV provides a security analysis of SRDV and shows that the countermeasures it employs ensures that attackers cannot manipulate or disrupt the computation and effective use of routes. Section V presents the results of simulation experiments to illustrate that SRDV attains the same or better efficiency than traditional nonsecured MANET routing protocols (AODV, DSR, OLSR) in the absence of attacks, and that its combination of end-to-end verification and path diversity with digital signatures and hash chains successfully defend against attacks by independent or colluding attackers.

[1]This work was partially sponsored by the U.S. Army Research Office under grant W911NF-05-1-0246, by the National Science Foundation under grant CNS-0435522, by DARPA through Air Force Research Laboratory (AFRL) Contract FA8750-07-C-0169, and by the Baskin Chair of Computer Engineering. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Defense Advanced Research Projects Agency or the U.S. Government.

978-1-4244-4581-3/09/$25.00 ©2009 IEEE

II. Previous Work

Previous work on secure routing for MANETs has depended on mechanisms that compromise scalability of the routing protocol, or that leave routing vulnerable to significant attacks. Hu et al [3] propose the *Secure Efficient Ad hoc Distance vector* protocol (SEAD) as an enhancement of the *Destination-Sequenced Distance-Vector* (DSDV) wireless ad hoc network routing protocol [11]. SEAD's primary enhancement over DSDV is the use of hash chains to authenticate the source of the update, and to secure the metric and sequence numbers contained in the update. The limitations lie in its efficiency and effectiveness as a routing protocol. It inherits the topology-driven routing model which as not as good a match for MANETs as on-demand routing protocols. In addition, the use of metrics updated by each hop in the network is susceptible to manipulation.

Several solutions requiring path information (based on DSR [6]) have been proposed. Ariadne [4] secures DSR routing using a number of mechanisms that, ultimately, allow the source of the request to verify that the request traversed a list of nodes given in the request, and that this list is the same seen by the target (destination) node when it received the route request. The approach taken secures the data plane at the cost of extensive signaling and bandwidth but data packets are still vulnerable to attack.

Eircksson et al [2] propose the new *Secure Probabilistic Routing* (Sprout) protocol for secure routing in wireless networks, with the specific goal of protecting against colluding attackers. Sprout is a link-state protocol that uses probabilistic route generation and selection with end-to-end route performance feedback to secure the routing function. Probabilistic route generation and selection results in an inherently multi-path routing solution. The strength of Sprout is that it tends to find and use shorter routes exhibiting high delivery ratios over time, even in the context of compromised and colluding nodes. Its primary limitation is a dependency on a topology-driven routing model, which is not a good match for MANETs.

Sanzgiri et al [15] propose the new *Authenticated Routing for Ad hoc Networks* (ARAN) protocol for secure routing in ad hoc networks. ARAN is an on-demand routing protocol that uses hop-by-hop authentication of all routing messages and end-to-end authentication of route discovery messages. The strength of ARAN is that it is a simple protocol that ensures the authenticity and integrity of routing messages, and uses an un-spoofable, end-to-end metric (delay of route signaling) for ensuring loop freedom and for use in route selection. However ARAN, like other protocols which use only a single unicast RREP, are particularly vulnerable to attackers dropping this RREP leading to denial of service attacks.

A number of solutions [9], [16] have been proposed for securing routing in wired, non-mobile environments that derive from early work by Perlman [12]. In these solutions the routing computation is secured with the digital signature of link state information by the node originating the routing update containing the link information. Receiving nodes validate updates before using them for their local computations. The limitations of this solution, discussed in [16], is that compromised routers can advertise fabricated links, allowing arbitrary manipulation of the forwarding topology. One possible solution, mentioned in [16], is the use of authentication of each link by a routing authority for use in verifying the validity of a link advertisement, but his solution is clearly not viable for MANETs.

TABLE I
Notation

Notation	Meaning
S	Source Address of a data flow
D	Destination Address of a data flow
s_X	Node X's secret (hash seed)
SN_X	Current Sequence Number of node X
$H_X(.)$	Node X's hash function
$H_X^t(s)$	Secret s, hashed t times using $H_X(.)$
$D_X(A)$	The distance (hop count) from X to A

III. SRDV

The goal of SRDV is to efficiently compute and use the shortest un-compromised paths available for the transmission of data through a network.

A. Security Model

We assume a *security association* between each node in a network, which can be instantiated with public/private keys, digital certificates or any other means of authentication. The use of such mechanisms have been studied extensively in the context of MANET environments and many solutions have been presented including the certificateless scheme of Zhang et. al. [17] and the on demand approach of Li et. al. [8]. Knowing the additional cost, we argue the necessity of authentication because without authentication, any malicious node can perpetually masquerade as the destination and this can lead to an unsolvable denial of service attack. We assume that the sources and destinations of data flow are not adversaries and that there exists a path between the source and destination which does not contain any adversaries, otherwise secure routing would be impossible.

Control packets are divided into fixed and variable fields. The fixed fields are signed by the originator and are not modified by intermediate nodes. Control packets are only processed if the signature is authenticated.

B. Hash Chains

Each node X, has a unique, cryptographically secure hash function $H_X(.)$, such as MD5 or SHA-1, and generates a new random secret, s_X, each time it initiates a RREQ or RREP. It then calculates $H_i^d(s)$, where d is the maximum allowed length of a path. When necessary, a node can produce a new cryptographically secure hash function.

Control packets carry $H_X(.)$ and $H_X^d(s)$ in the fixed fields (which are digitally signed) and nodes are responsible for hashing the current hash value $H_X^t(s)$, where t is the number of hops from the source of the packet, in the variable field. Upon receiving a packet, the node checks the authenticity of

the packet using the digital signature. Once authenticated, the node then verifies the integrity of the hash value.

The use of the hash chain does not completely secure the hop count but it makes it more difficult to distort the topology.

C. Route Establishment and Maintenance

The signaling in SRDV is hybrid, in that path establishment is on demand and maintenance is proactive. When a node has data to send and no path, it initiates a route request (RREQ). This RREQ is flooded throughout the network. Intermediate nodes do not modify any of the fixed fields of the packet, just increases the hop count and hash the hash value. The source sequence number is used to ensure that each node transmits each RREQ at most once.

When the destination node receives a RREQ with a new sequence number it will issue a route reply (RREP). This RREP will be retransmitted by node X, as long as it satisfies the following equation which defines a *region of interest*:

$$D_S(X) + D_D(X) \leq D_S(D) + 2 + \delta \tag{1}$$

The value of δ is number of successive failed attempt of route discovery. The distance to the source and destination would be the number of hops traveled by the RREQ and RREP to the node respectively and the distance from the source to the destination $D_S(D)$ is stored in the RREP, and is determined by the destination based on the RREQ received.

As long as there are data packets in the flow, both the source and destination periodically initiate unsolicited RREPs serving to update the routing information.

D. Path Diversity and Data Forwarding

In a hostile environment, the probability of finding a secure path can be improved by routing data using multiple paths. If one path performs noticeably worse than another, it could be due to adversaries on or near that path. Bad performance can be attributed to benign causes as well, but neither case is desirable.

All the nodes are ordered with respect to hop count (an advertised metric) and bottleneck bandwidth (a measured characteristic) with hop count having priority and bandwidth being used to choose between nodes with the same hop count.

For simplicity, data is routed over two paths in our implementation of SRDV. The first path is the best, given the current ordering, and the second path is made by each node choosing its second-best path known to them. Each data packet carries a label to indicate which path should be used.

It is relatively easy for malicious nodes to manipulate the signaling so that they appear on the best path, especially if they are colluding with each other. However, it is far more difficult to appear in the second best path especially in a dynamic topology. Therefore this approach, although a very simple form for multi-path routing, can significantly improve the performance when combined with load balancing. Being on the best path will be of little advantage to adversaries if most of the data packets are routed through an alternate path with better performance.

E. Link Failures

When an intermediate node with a data packet experiences a link failure, it tries to route through a different neighbor (as long as it is a successor based on the current ordering of the nodes). If there is no such neighbor, the node changes its hop count to infinity and broadcasts an update to alert its neighbors of this change. Once neighboring nodes update their routing table based on this information, they in turn check for an alternate paths which it will use to route data. A neighbor with no feasible path changes its hop count to infinity and alerts its own neighbors. If this percolates to the source node, a new RREQ is initiated with an increased sequence number. Nodes that have reset their distances to a destination to infinity can change their hop count to non-infinite values only upon receiving a RREP with a sequence number higher than the local sequence number value they stored.

F. QoS Probing

Nodes take measurements of delay and bandwidth to evaluate the validity of the advertised ordering (hop counts) with the actual performance of paths. Destination nodes immediately reply to RREQs by issuing RREPs. Hence, the time elapsed from the instant when a RREQ is initiated to the time the first RREP to it is received gives a good estimate of the end-to-end delay (t^o_{rtt}). The source node randomly selects data packets for which it will measure end-to-end delay.

If the delay experienced by data packets is significantly larger, it is indicative of a possible attack and the path is avoided.

The use of packet pairs to estimate the bottleneck bandwidth has been extensively studied [1], [13] and more complex schemes have been since presented which use a packet train or improved queuing [14]. Periodically, instead of initiating a single proactive RREP, the destination initiates two successive RREPs, with consecutive sequence numbers. Nodes measure the inter-arrival time of these packets and forward both packets.

G. End-to-End Feedback and Load Balancing

An important indication of performance is the number of packets delivered. An updated value for the number of packets received from each path is sent to the source in the periodic RREPs. SRDV then uses this feedback and QoS measurements to perform load balancing on the available paths.

The performance of each path determines the fraction of packets sent along the path. Paths which deliver the greater fraction of packets are favored as are those with lower end-to-end data packet delivery time. If a node suspects, based on measurements and feedback, that one path is under attack, it can set a blacklist flag in the next periodic RREP it issues. Upon receiving this notification a node ignores all overheard packets from its current best or second-best successor depending on the flag. This allows for the formation of different paths the next time the ordering is updated.

IV. Protocol Security Analysis

The goals in securing SRDV are to ensure that an attacker cannot manipulate or disrupt the routing computation. Manipulation of the routing computation allows an attacker to control the forwarding topology such that traffic is forwarded over paths containing the attacker. Given access to traffic, an attacker can launch denial of service, disclosure, or hijacking attacks on network sessions. Disruption of the routing computation results in various degrees of denial of service. The fundamental security requirements needed of a routing protocol to meet these goals are the authentication and authorization of nodes participating in the routing computation and the integrity and availability of the routing computation.

A. Route Discovery and Maintenance

Route requests and replies can be deleted, fabricated, modified, or replayed. *Deleting* a route request or reply prevents the discovery of an alternative path in the network. However, the path eliminated by this attack is a path that, by definition, contains an attacker. Furthermore, to have the ability to delete a routing message, the attacker must either be a compromised link or router. *Therefore, the best response is to allow this attack and avoid a known compromised path.*

Fabricating a route request or reply results in resource consumption from the unauthorized flood of the request throughout either the network or region of interest, or the manipulation of the forwarding topology by an attacker masquerading as another source in the network. *Authentication of the fixed fields in the request or reply at each hop are used as the countermeasure to this threat.* It is assumed that the encryption process is secure and digital signatures cannot be forged thus SRDV would be immune to this type of attack.

Replay of a route request or reply can result in the same compromises described above for fabrication. *The countermeasure to this threat is the use of a sequence numbers in route requests and replies.* Since the sequence number is in the fixed field, and therefore signed, it cannot to tampered with my intermediate nodes to make old packets appear new.

Lastly, *modification* of the hop count by an intermediate router results in the use of sub-optimal forwarding paths that include the attacker. This results in some unnecessary resource consumption, and the potential denial of service or disclosure of traffic described above. *Secure hash chains (Section III-B) are used as the countermeasure to this threat.*. This would be the most effective form of attack against SRDV, but we shall prove that adversaries are unable to prevent route discovery in SRDV regardless of their behavior.

Theorem 4.1: Let $L_S^{t^n}$ denote the length of the shortest path $(N_1, N_2 ... N_k)$ between N_1 and N_k such that each N_i is not an adversary, at a time n. Let $L_R^{t^n}$ denote the diameter of the region of interest between N_1 and N_k. Then $L_S^{t^n} \leq L_R^{t^n}$ is a sufficient, but not necessary, condition to ensure that packets flooded in the region of interest by N_1 will be received by N_k and vice versa.

Proof: The proof is by induction on the length of the path $(N_1, N_2 ... N_k)$.

For a path of length one, N_1 transmitted the packet, and N_2 is a neighbor of N_1, therefore N_2 would have received the packet (from N_1), so it is true for a path length of one.

Now assume it is true for a path of length j, where $0 \leq j \leq L_R^{t^n}$. Since $j = L_S^{t^n} \leq L_R^{t^n}$, N_j must be in the region of interest and is not an adversary so N_j would retransmit the packet. Therefore the packet would be received at N_{j+1}.

The same argument can be used to prove the reverse direction, any packet flooded in the region of interest of N_k would be received by N_1. The condition is not necessary, because packets can arrive at N_k from N_1 through a possibly shorter path that contains adversaries.

■

Theorem 4.2: Adversaries cannot indefinitely prevent route discovery in SRDV.

Proof: To prevent route discovery between source N_1 and destination N_k, node N_1 cannot receive a RREP for a RREQ it issued. There are two possible cases:

1) The RREQ never arrived at the destination.
2) The RREQ arrived at the destination D, but the RREP never arrived at the source of the RREQ.

For the first case, the diameter of the region of interest is the diameter of the network therefore $L_S^{t^n} \leq L_R^{t^n} =$ *Network Diameter*, and by Theorem 4.1, the RREQ would arrive at the destination. Therefore, this case is not possible.

Consider the second case. If N_1 did not receive the RREP, it will retry the RREQ and we can be certain this RREQ will reach N_k. At this point, N_k would set the diameter of the region of interest to $L_R^{t^{n+1}} = L_{RREQ}^{t^{n+1}} + 2 + \delta$ where δ is the number of successive retries, and $L_{RREQ}^{t^{n+1}}$ is the distance traveled by the route request, at time (n+1). Since $L_{RREQ}^{t^{n+1}} \geq 0$, we have $L_R^{t^{n+1}} \geq \delta + 2$.

We note that eventually, $L_S^{t^{n+\delta}} \leq L_R^{t^{n+\delta}}$ after some number of retries (since the value of δ, and therefore the diameter of the region of interest, will increase with each successive failure) and at this point, by Theorem 4.1, we can be assured that the RREP will arrive at N_1 at which point in time route discovery would have taken place. Thus it is impossible to prevent route discovery in SRDV.

■

B. Securing Data Delivery

Securing route discovery and route maintenance is essential to successfully routing data, but by itself would prove to be an insufficient solution. The routing protocol should be able to detect and avoid malicious attacks on data packets. Some nodes may behave correctly during the route discovery phase but then drop data packets routed through them, or they may use a wormhole, which is undetectable in the route discovery phase, to force packets to be routed through them and then perform denial of service or disclosure attacks. The most reliable means to detect such attacks on data packets is to through end-to-end feedback. Corollary 1 proves that

the performance feedback reaches the source node, and this is crucial to detecting attacks. Adversaries may be able to temporarily disrupt the feedback mechanism, but this action cannot be maintained indefinitely.

Corollary 1: Feedback information from the destination eventually arrives at the source.

Proof: A destination node N_k can determine if its update packets (with feedback information) arrive at the destination based on the sequence number for N_k in the update from the source N_1 or the lack of such an update. Once the destination determines the updates are not being received at the source, it can increase the diameter of the region of interest until update packets are delivered and from Theorem 4.2 it follows that this must happen. ■

Parameter	Value
Simulation Time	900s
Number of Nodes	100
Simulation Area	1000m x 1000m
Node Placement	Uniform
Mobility Model	Random Waypoint
Min-Max Speed	1-10m/s
Pause Time	30s
Propagation Model	Two-ray
Physical Layer	802.11
Antenna Model	Omnidirectional
MAC Protocol	802.11 DCF
Data Source	CBR
Number of Packets per Flow	800
Packet Rate	4 packets per second
Packet Size	512 Bytes
Node Density	0.001 nodes/m^2

TABLE II
SIMULATION PARAMETERS

V. SIMULATIONS

We use simulations to show that, in the absence of attacks, SRDV can be as effective as proactive and reactive routing protocols, while delivering significantly more packets and defending against a variety of attacks in hostile environments.

We compare the performance of SRDV to that of AODV, DSR, OLSR and ARAN.In uSRDV we remove the multipath capabilities, the end-to-end feedback and measurements, the cryptography and the hash chains from SRDV. This leaves a basic, single-path hybrid routing protocol. Using this as a base measure, we can highlight the cost of our security mechanisms.

Two scenarios were used and the parameters are summarized in Table II. The first of these was designed to test the performance of the protocols in a dynamic environment with volatile links. This choice of parameters satisfies the minimum standards for rigorous MANET protocol evaluation as prescribed in [7], because it results in an *average shortest path hop count* [7] of 4.03 and *average network partitioning* [7] of 3.9%. The radio range in this scenario was 150m. The second scenario uses a greater radio range, 200m, to add more stability to the links and create more multi-path opportunities.

Each experiment was repeated 50 times with random node placement and mobility. In each experiment, there were 10 CBR sources, which started generating packets at a random time to a randomly chosen destination.

Three metrics were used to evaluate and compare the performance of the protocols. Delivery ratio is the fraction of packets that arrive at the corresponding destination by the end of the simulation. Latency is the average end-to-end delay experienced by the data packets. Net load is the number of control packets (RREQs, RREPs, RERRs, Hellos, and TC messages) which were initiated or forwarded, normalized by the number of data packets sent. This last metric gives an indication of the average number of control packets needed to send a packet from the source to the destination.

A. Performance with No Adversaries

The first set of experiments aims to show the effectiveness of the SRDV protocol in an environment where there are no attackers. The simulation results for the six routing protocols tested are summarized in Table III, where the mean and a 95 percent confidence interval are given.

Based on these results, it is evident that both uSRDV and SRDV deliver more packets than the other protocols while incurring significantly less overhead than AODV and OLSR. SRDV incurs greater delay than AODV mainly because it attempts to use alternate routes which may be broken, or non existent and percolation of this information takes a longer time to the source. More opportunities for nodes to find multiple successors in Scenario B, which leads to better performance.

B. Performance with Independent Adversaries

In this set of simulations, we allow for 30% of the nodes to be attackers on average, but each acts independently of the others. 20% of nodes in the network alter the hop count in RREPs by either increasing or decreasing it by up to three hops with the exact amount being random. Half of these nodes (which modify hop count) also drop all data packets routed through them. A disjoint 10% of nodes in the network drop all RREPs. This results in a wide variety of attacks with the goal of either capturing data packets or thwarting the routing process. There is no merit in simulating fabrication and masquerading attacks, because the digital signatures render these attacks futile.

For comparison, we use an authenticated form of AODV (which we call aAODV), which requires nodes to sign packets they initiate. Using AODV is not adequate, because it simply becomes inoperable under fabrication attacks, which is also the case for DSR and OLSR. Furthermore, since aAODV and SRDV utilize these same authentication services, the difference in performance between the two protocols can be attributed to the path diversity and the end-to-end feedback mechanisms that we want to highlight.

While aAODV and ARAN are less susceptible to hop count manipulation since the RREPs are sent back long the quickest path, they are more vulnerable to attackers which forward RREQs but then drop RREPs, especially if these attackers lie on the fastest path from the source to the destination. Such attacks can result in extensive flooding and denial of service.

TABLE III
SIMULATION RESULTS

Scenario A			
	Delivery Ratio	Latency	Net Load
No Adversaries			
AODV	0.60±0.10	0.086±0.037	14.4±5.3
DSR	0.14±0.10	18.5±15.9	5.0±1.2
OLSR	0.30±0.08	0.072±0.015	67.5±1.2
ARAN	0.53 ± 0.09	0.21 ±0.11	24.7 ± 5.0
uSRDV	0.78±0.10	0.147±0.104	7.9 ±2.7
SRDV	0.77 ± 0.07	0.132 ± 0.06	8.7 ± 2.2
Independent Adversaries			
aAODV	0.29±0.11	0.032±0.012	8.8±2.2
ARAN	0.33± 0.12	0.26 ± 0.11	10.2 ±1.5
uSRDV	0.28±0.08	0.283±0.163	3.9 ±0.8
SRDV	0.45 ± 0.09	0.112 ± 0.054	5.0 ± 1.3
Wormhole Attacks			
aAODV	0.42±0. 11	0.043±0.018	8.8±1.1
ARAN	0.57 ± 0.04	0.31 ± 0.10	22.1 ± 3
uSRDV	0.68±0.11	0.127±0.048	10.0 ±1.6
SRDV	0.79 ± 0.09	0.087 ± 0.026	7.3 ± 2.4
Scenario B			
No Adversaries			
AODV	0.90 ± 0.03	0.072 ± 0.015	5.04 ± 1.31
DSR	0.14 ± 0.04	42.7 ± 12.9	2.65 ± 0.34
OLSR	0.71 ± 0.04	0.104 ± 0.021	17.2 ± 0.2
ARAN	0.91 ± 0.07	0.11 ± 0.06	3.0 ± 0.9
uSRDV	0.98 ± 0.03	0.067 ± 0.047	1.92 ± 0.20
SRDV	0.95 ± 0.03	0.056 ± 0.018	2.92 ± 0.60
Independent Adversaries			
aAODV	0.48 ± 0.15	0.030 ± 0.008	5.6 ± 1.6
ARAN	0.51 ± 0.10	0.22 ± 0.09	5.7 ± 2.0
uSRDV	0.37 ± 0.13	0.156 ± 0.153	1.9 ± 0.5
SSRDV	0.59 ± 0.09	0.053 ± 0.023	3.3 ± 0.6
Wormhole Attacks			
aAODV	0.58 ± 0.18	0.050 ± 0.029	5.6 ± 1.7
ARAN	0.88 ± 0.06	0.11 ± 0.05	8.9 ± 4.1
uSRDV	0.96 ± 0.03	0.044 ± 0.012	3.2 ± 0.7
SRDV	0.91 ± 0 .04	0.053 ± 0.02	5.1 ± 0.1

In SRDV, the RREP is sent of several paths and has a greater chance of arriving at the source.

The aAODV protocol has no protection against malicious nodes that forward control packets but drop data packets. Given sufficient multipath options, SRDV sends the greater number of data packets along the more successful routes. However, the ordering in SRDV can be compromised, which could be another reason why packets are not delivered. The results in Table III show the performance of the protocols. The significant overhead incurred by aAODV demonstrates the advantages of the SRDV's security philosophy.

C. Performance with Colluding Adversaries

One form of attack that has received significant attention lately is wormhole attacks [5] and we demonstrate that SRDV is capable of detecting and defending against this attack.

Of the 100 nodes in the network, 10 were randomly join and were then divided into five pairs. A wired link with three times the latency of a wireless link was used to connect the nodes in each pair. The nodes can then use this link to tunnel packets from one point in the network to another. Each of these 10 nodes then drop all data packets they receive.

The results in Table III show that the use of end-to-end feedback and path diversity used in SRDV helps improve routing in the face of wormhole attacks, in fact the wormholes have very little impact on SRDV but significantly degrade the performance of aAODV. In Scenario B, because of the smaller network diameter, wormhole attacks have reduced effectiveness and this is reflected in the results.

VI. CONCLUSIONS

We have argued that previous solutions for securing routing in MANETs have significant limitations, and presented SRDV as an instantiation of an approach based on end-to-end verification of path characteristics and the use of path diversity. SRDV addresses all of the security problems identified with prior approaches for secure routing in MANETs. We showed through simulation experiments that SRDV is at least as efficient as traditional MANET routing protocols in the absence of attacks, and that it attains better performance under attacks than protocols that simply rely on single-path routing and the authentication of control packets.

REFERENCES

[1] J.-C. Bolo. End-to-end packet delay and loss behavior in the internet. In *ACM SIGCOMM*, 1993.

[2] J. Ericksson, M. Faloutsos, and S. V. Krishnamurthy. Routing amid colluding attackers. In *Proc. ICNP*, 2007.

[3] Y.-C. Hu, D. B. Johnson, and A. Perrig. Sead: secure and efficient distance vector routing for mobile wireless ad hoc networks. *Ad Hoc Networks*, 1:175–192, 2003.

[4] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In *Wireless Networks*, volume 11, pages 21–38, 2005.

[5] Y.-C. Hu, A. Perrig, and D. B. Johnson. Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):370–380, February 2006.

[6] D. B. Johnson, D. A. Maltz, and J. Broch. Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks. In C. E. Perkins, editor, *Ad Hoc Networking*, chapter 5, pages 139–172. Addison-Wesley, 2001.

[7] S. Kurkowski, T. Camp, and W. Navidi. Minimal Standards for Rigorous MANET Routing Protocol Evaluation. *Technical Report MCS 06-02, Colorado School of Mines*, 2006.

[8] R. Li, J. Li, P. Liu, and H.-H. Chen. On-demand public-key management for mobile ad hoc networks. *Wireless Commmunications and Mobile Computing*, 6(3):295–306, 2006.

[9] S. L. Murphy. Digital signature protection of the ospf routing protocol. In *Proceedings Symposium on Network and Distributed System Security*, February 1996.

[10] P. Papadimitratos and Z. Haas. Secure routing for mobile ad hoc networks. *ACM Mobile Computing and Communications Review (MC2R*, 2003.

[11] C. E. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. In *Proceedings SIGCOMM '94*, pages 234–244, August 1994.

[12] R. Perlman. *Network Layer Protocols with Byzantine Robustness*. PhD thesis, Massachusetts Institute of Technology, October 1988.

[13] R. Prasad, C. Dovrolis, M. Murray, and K. Claffy. Bandwidth estimation: metrics, measurement techniques, and tools. *IEEE Network*, 2003.

[14] S. ryong Kang, X. Liu, and M. D. D. Loguinov. Packet-pair bandwidth estimation: Stochastic analysis of a single congested node. In *IEEE Internation Conference on Network Protocols*, 2004.

[15] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. Belding-Beyer. A secure routing protocol for ad hoc networks. In *Proceedings International Conference on Network Protocols*, 2002.

[16] B. R. Smith, S. Murthy, and J. Garcia-Luna-Aceves. Securing distance-vector routing protocols. In *Proceedings Symposium on Network and Distributed System Security*, February 1997.

[17] Y. Zhang, W. Liu, and Y. Fanf. Securing mobile ad hoc networks with certificateless public keys. *IEEE Transactions on Dependable and Secure Computing*, 3(4), 2006.