Journal of Computer Applications ISSN: 0974 – 1925,
Volume-5, Issue EICA2012-4, February 10, 2012

Improving CA-AOMDV Protocol Against Blackhole Attacks

Sherril Sophie Maria Vincent
ME. Computer Science
PITAM, Thiruvallur
E-mail: sherrilvincent@hotmail.com

Thamba Meshach W
ME. Computer Science
PITAM, Thiruvallur
E-mail: meshacjc@gmail.com

Abstract - Mobile ad hoc networks are infrastructure less network where the nodes themselves are responsible for routing the packets. The dynamic topology of MANETs allows nodes to join and leave the network at any point of time. Due to security vulnerabilities of the routing protocols, wireless ad hoc networks are not protected against the attack of malicious nodes. One of these attacks is the Black hole Attack. In the conventional scheme a channel aware feature is added on the AOMDV Protocol to overcome the channel fading. However this scheme does not provide any security against the Black hole Attack. This paper contributes a mechanism that generates randomized multipath route which is circumventing black holes. The security and energy performance are analytically investigated. Extensive simulations are performed to verify and validate the mechanism.

Keywords: *Black Hole Attack, Mobile ad hoc networks, channel adaptive routing, Randomized multi-path routing.*

I. INTRODUCTION

Mobile Ad Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self-configuration ability, they can be deployed urgently without the need of any infrastructure. A major performance constraint comes from path loss and multipath fading. Many MANET routing protocols exploit multi hop paths to route packets. The probability of successful packet transmission on a path is dependent on the reliability of the wireless channel on each hop. Rapid node movements also affect link stability, introducing a large Doppler spread, resulting in rapid channel variations.

Channel-aware version of the AOMDV routing protocol. The key aspect of this enhancement, which is not addressed in other work, is that we use specific, timely, channel quality information allowing us to work with the ebb-and-flow of path availability. This approach allows reuse of paths which become unavailable for a time, rather than simply regarding them as useless, upon failure, and discarding them. The channel average nonfading duration (ANFD) as a measure of link stability, combined with the traditional hop-count measure for path selection. The protocol then uses the same information to

predict signal fading and incorporates path handover to avoid unnecessary overhead from a new path discovery process. The average fading duration (AFD) is utilized to determine when to bring a path back into play, allowing for the varying nature of path usability instead of discarding at initial failure. This protocol provides a dual attack for avoiding unnecessary route discoveries, predicting path failure leading to handoff and then bringing paths back into play when they are again available, rather than simply discarding them at the first sign of a fade.

Security in Mobile Ad Hoc Network is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of the its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

MANETs must have a secure way for transmission and communication and this is quite challenging and vital issue as there is increasing threats of attack on the Mobile Network. Security is the cry of the day. In order to provide secure communication and transmission engineer must understand different types of attacks and their effects on the MANETs. Further, a detailed theoretical analysis of the lifetimes of both protocols and expressions for performance with respect to routing.

II. REVIEW OF AOMDV

The key distinguishing feature of AOMDV over AODV is that it provides multiple paths to nd. These paths are loop free and mutually link-disjoint. AOMDV uses the notion of advertised hop-count to maintain multiple paths with the same destination sequence number. In both AODV and AOMDV, receipt of a RREQ initiates a node route table entry in preparation for receipt of a returning RREP. In AODV, the routing table entry contains the fields:

<destination IP address,
destination sequence number,
next-hop IP address,
hop-count,
entry expiration time>,

where entry expiration time gives the time after which, if a corresponding RREP has not been received, the entry is discarded. In AOMDV, the routing table entry is slightly modified to allow for maintenance of multiple entries and multiple loop-free paths. First, advertised hop-count replaces hop-count and advertised hop-count is the maximum over all paths from the current node to nd, so only one value is advertised from that node for a given

destination sequence number. Second, next-hop IP address is replaced by a list of all next-hop nodes and corresponding hop-counts of the saved paths to nd from that node, as follows:

<destination IP address,
destination sequence number,
advertized hop-count,
route list: {(next hop IP 1, hop-count 1),
(next hop IP 2, hop-count 2), . . . },
entry expiration time>.

To obtain link-disjoint paths in AOMDV, nd can reply to multiple copies of a given RREQ, as long as they arrive via different neighbors.

III. CHANNEL AWARE AOMDV PROTOCOL

Route discovery in AOMDV results in selection of multiple loop-free, link-disjoint paths between ns and n_d, with alternative paths only utilized if the active path becomes unserviceable. One of the main shortcomings of AOMDV is that the only characteristic considered when choosing a path is the number of hops. Path stability is completely ignored. Thus, selected paths tend to have a small number of long hops meaning that nodes are already close to the maximum possible communication distance apart, potentially resulting in frequent link disconnections. In CA-AOMDV, we address this deficiency in two ways. In the route discovery phase, we utilize the ANFD metric, of each link as a measure of its stability. In the route maintenance phase, instead of waiting for the active path to fail, we preempt a failure by using channel prediction on path links, allowing a handover to one of the remaining selected paths. This results in saved packets and consequently smaller delays. The routing table structures for each path entry in AOMDV
and CA-AOMDV are shown in Table 1.

Table 1
Comparison of Routing Table Entry Structures in AOMDV and CA-AOMDV

AOMDV routing table	CA-AOMDV routing table
destination IP address	destination IP address
destination sequence number	destination sequence number
advertised hop-count	advertised hop-count
	$\mathcal{D}_{min}$
path list {(next hop IP 1,hop-count 1), (next hop IP 2,hop-count 2),$\cdots$}	path list {(next hop 1,hop-count 1,$\mathcal{D}_1$), (next hop 2,hop-count 2,$\mathcal{D}_2$),$\cdots$}
	expiration timeout
expiration timeout	handoff dormant time

3.1 Route Discovery in CA-AOMDV

Route discovery in CA-AOMDV is an enhanced version of route discovery in AOMDV, incorporating channel properties for choosing more reliable paths. CA-AOMDV uses the ANFD as a measure of link lifetime. The path duration, D, is recorded in the RREQ, updated, as necessary, at each intermediate node. Thus, all information required for calculating the ANFD is available via the RREQs, minimizing added complexity. Similarly, to the way the

longest hop path is advertised for each node in AOMDV to allow for the worst case at each node, in CA-AOMDV the minimum D over all paths between the given nodes, n_i, and n_d, is used as part of the cost function in path selection.

3.2 Route Maintenance in CA-AOMDV

In mobile environments, it is necessary to find efficient ways of addressing path failure. Using prediction and handoff to preempt fading on a link on the active path, disconnections can be minimized, reducing transmission latency and packet drop rate.

Route maintenance in CA-AOMDV takes advantage of a handoff strategy using signal strength prediction, to counter channel fading. When the predicted link signal strength level falls below a network specific threshold, the algorithm swaps to a good-quality link. The fading threshold is chosen so as to provide robustness to prediction errors. The presence of multiple users experiencing independent channel fading means that MANETs can take advantage of channel diversity, unlike data rate adaptation mechanisms such as Sample Rate.

All nodes maintain a table of past signal strengths, recording for each received packet, previous hop, signal power and arrival time. However, this will depend on the packet receipt times compared with the specified discrete time interval, _t. If packets are received at time intervals greater than _t, sample signal strengths for the missed time intervals can be approximated by the signal strength of the packet closest in time to the one missed. If packets are received at intervals of shorter duration than _t.

3.3 Handoff Trigger

Route handoff is triggered when a link downstream node predicts a fade and transmits a HREQ to the uplink node. Let T_R be the transmission range, assumed to be the same for all nodes, let $\acute{R}(t)$ be predicted signal strength at time t and recall Rth as the fade prediction threshold. If the prediction at $t0 + \psi$ is above Rth while that at $t0 + 2\psi$ is below, the maximum transmitter velocity V_t max ensuring signal strength above Rth at $t0 + \psi$, is determined. If a fade is predicted at either time, the receiver checks whether the link is at breaking point with respect to distance. The HREQ registers the following fields: source IP address, destination IP address, source sequence number, fade interval index, long term fading indicator, AFD, and Vt max.

3.4 Handoff Table to Avoid Duplicate HREQs

In addition to the routing table described in Table 1, each node maintains a local handoff table. Each entry includes: source IP address, source sequence number, destination IP address, and expiration timeout. Expiration timeout indicates when a path is expected to be available again (out of the fade) and is set to the maximum AFD of all currently faded links with paths through that node to particular ns. Note that this is similar to the way advertised hop-count is set to the maximum number of hops for any path going through a node for a particular ns in AOMDV. Whenever a node receives a HREQ targeting particular ns, it checks its handoff table for an entry relating to that ns. The handoff is updated if no entry exists for that ns, if the new HREQ has a longer AFD or if the existing entry is stale due to

the expiration timeout having expired. If any unexpired entry is found for that ns with the same or higher source sequence number, the HREQ is dropped.

3.5 Forwarding the HREQ

Any node receiving a non-duplicate HREQ checks for alternative paths to nd. If not, as for the case of node D in Fig. 2, it propagates the HREQ. Otherwise, if it has one or more "good" alternative paths to the nd, it marks the fading path indicated in the HREQ as dormant, setting the handoff dormant time in its routing table entry for that path to the AFD recorded in the HREQ. The HREQ is then dropped. If a fade is predicted on the active path, a non-dormant alternative path to nd is then adopted prior to the onset of link failure. For example, if node C in Fig. 2 receives a HREQ from node D, it marks the path with next hop ¼ D as dormant, and adopts the path with next hop ¼ E. The dormant path is retained for use when the fade is over, reducing path discovery overhead.

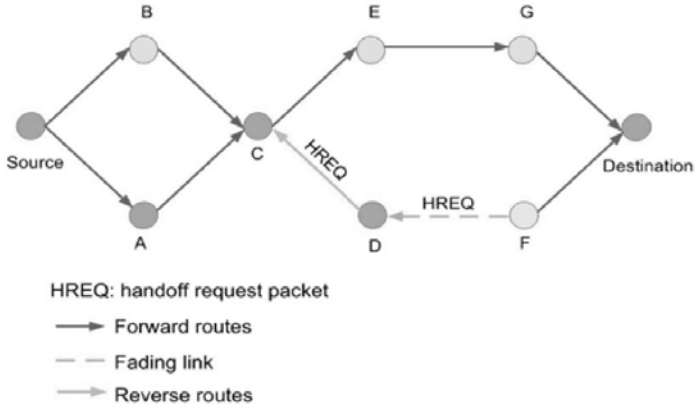

Figure 1: Handoff in CA-AOMDV

IV. RANDOMIZED MULTI-PATH DELIVERY

As illustrated in Figure 2, we consider a 3-phase approach for secure information delivery in a MANETs: secret sharing of information, randomized propagation of each information share, and normal routing (e.g., minhop routing) toward the sink. More specifically, when a sensor node wants to send a packet to the sink, it first breaks the packet into *M* shares according to a (*T;M*)-threshold secret sharing algorithm, e.g., Shamir's algorithm. Each share is then transmitted to some randomly selected neighbor. That neighbor will continue to relay the share it has received to other randomly selected neighbors, and so on. In each share, there is a TTL field, whose initial value is set by the source node to control the total number of random relays. After each relay, the TTL field is reduced by 1. When the TTL value reaches 0, the last node to receive this share begins to route it towards the sink using min-hop routing. Once the sink collects at least *T* shares, it can reconstruct the original packet. No information can be recovered from less than *T* shares.

The effect of route deperssiveness on bypassing black holes is illustrated in Figure 3, where the dotted circles represent the ranges the secret shares can be propagated to in the random propagation phase. A larger dotted circle implies that the resulting routes are geographically more dispersive. Comparing the two cases in Figure 2, it is clear that the routes of higher

dispersiveness are more capable of avoiding the black hole. Clearly, the random propagation phase is the key component that dictates the security and energy performance of the entire mechanism.

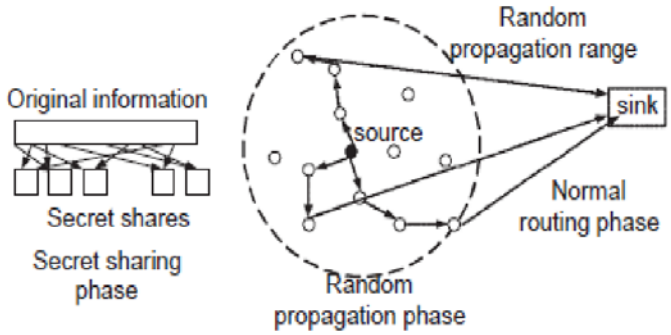

Figure 2: Randomized Dispersive Routing in a WSN.

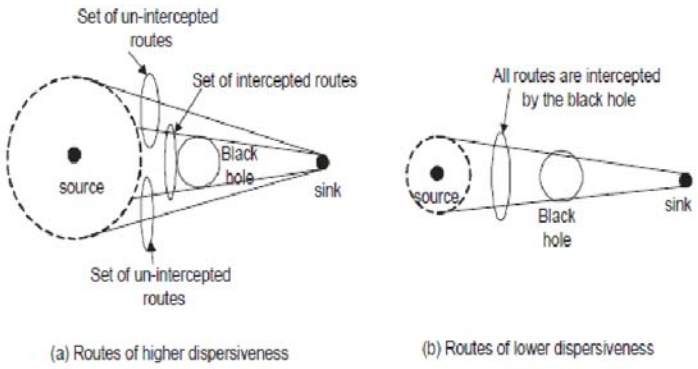

Figure 3: Implication of Route Dispersiveness on Bypassing the Black Hole.

V. PERFORMANCE EVALUATION

Figure 4 plots the packet interception probability as a function of the black hole size under various combinations of N and M. It is clear that the message is more likely to be intercepted when the black hole becomes larger, but increasing either N or M helps to reduce the interception rate. It is also noted from the crossing between curves that there is no absolute winner between increasing N and increasing M to reduce the interception probability. In the low-interception-probability regime, increasing M gives better performance, while in the high-interception regime, increasing N becomes better. This can be explained as follows: An increase in N helps to propagate information shares more dispersively, thus reducing the interception probability of each share (PI). Increasing M does not affect the interception probability of the share, but the black hole needs to collect more shares to recover a packet. It is clear the latter takes effect as the exponent while the former is on the base. When $PI << 1$, a larger exponent provides faster decay of the probability than reducing the base, and vice versa. We plot the packet interception probability as a function of the black hole location in

Figures 5. It is clear that the closer the black hole to the sink, the larger the interception probability. This is in line with the many to-one data collection paradigm in MANETs. For example, if the sink is compromised, then all packets will be intercepted by the adversary (no effective counter-attack measure exists in this case).

The Wanderer algorithm has poor energy performance, because it results in long paths. In contrast, the multi path routing scheme proposed in this paper are specifically tailored to security considerations in energy constrained MANETs. They provide highly dispersive random routes at low energy cost without generating extra copies of secret shares.

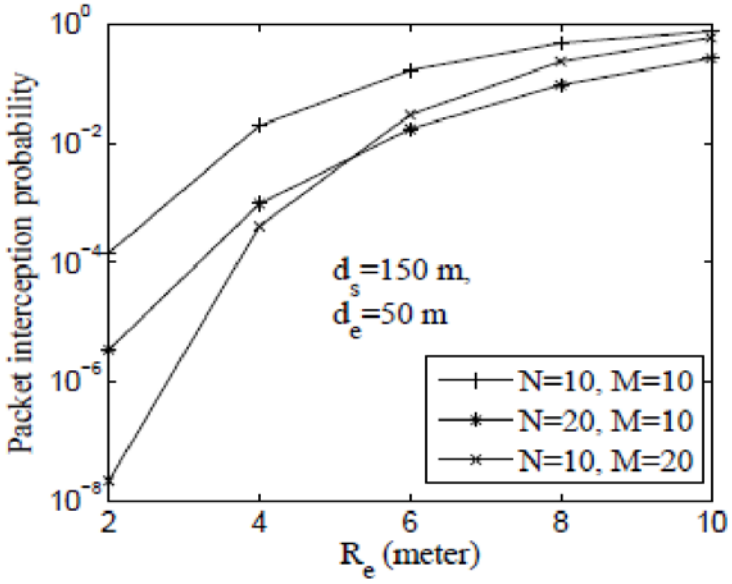

Figure 4: Packet Interception Probability vs. Black Hole Size

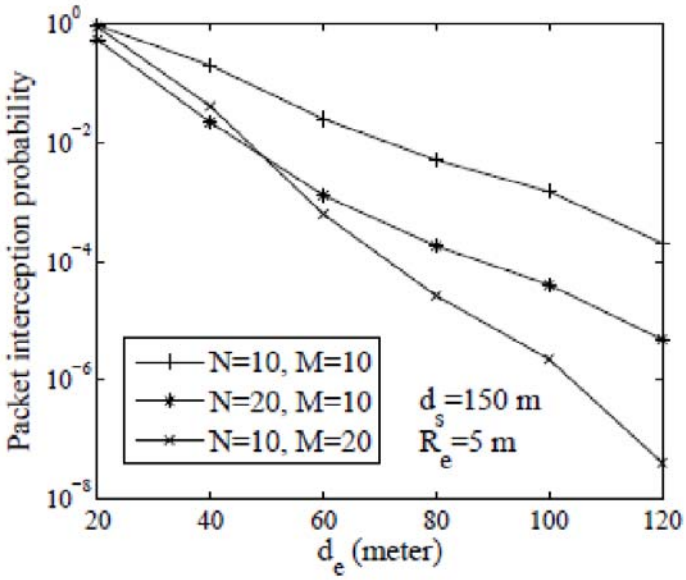

Figure 5: Packet Interception Probability vs. Black Hole Location

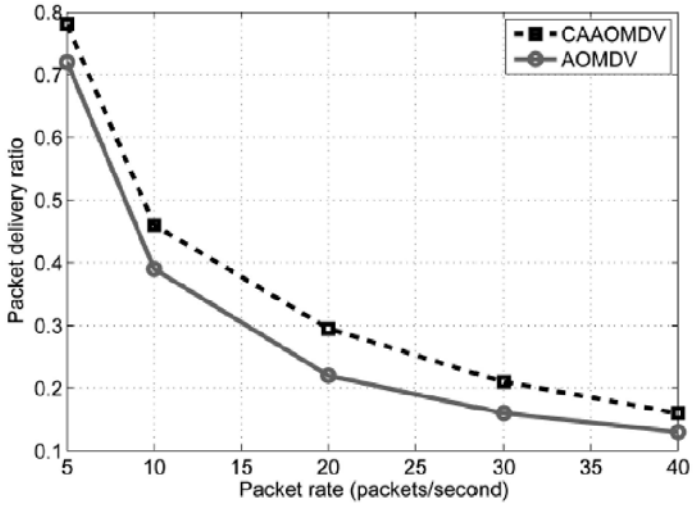

Figure 6: Packet Delivery Ratio Comparison between CA-AOMDV and AOMDV with Increasing Packet Rate

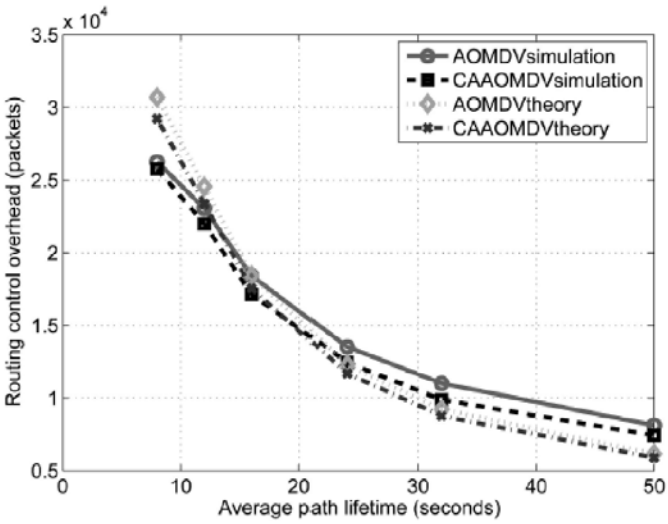

Figure 7: Routing Control Overhead Comparison of Theoretical and Simulated Results with Increasing Average Path Lifetime

VI. CONCLUSION

The major problems in mobile computing is channel fading and security issues in transmission of data packets .The paper proposes a channel adaptive scheme which overcomes the channel fading in addition to it a multi path propagation algorithm is proposed to overcome the back hole attack that is common in MANETs. The two metrics, Average Non fading metric and Average fading metric is calculated to keep track of fading and perform handoffs. The multi path propagation algorithm makes use of information shares that are split from the original information and dispersed in multiple paths. The packets are being delivered without packet loss.

REFERENCES

1. Biswas S. and Morris R., "ExOR: Opportunistic Multi-Hop Routing for Wireless Networks," ACM SIGCOMM Computer Comm. Rev., vol. 35, no. 4, pp. 133-144, Aug. 2005.
2. Pham P., Perreau S., and Jayasuriya A., "New Cross-Layer Design Approach to Ad Hoc Networks under Rayleigh Fading," IEEE J. Selected Areas in Comm., vol. 23, no. 1, pp. 28-39, Jan. 2005.
3. Vaidya B, Pyun Y. J., Park J A., and Han S.J.. Secure multipath routing scheme for mobile ad hoc network. In Proceedings of IEEE International Symposium on Dependable, Autonomic and Secure Computing, pages 163–171, 2007.
4. Charles E. Perkins, and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector (AODV) routing," Internet Draft, November 2002.
5. Ye Z., Krishnamurthy V., and Tripathi S.K., A framework for reliable routing in mobile ad hoc networks. In Proceedings of the IEEE INFOCOM Conference, volume 1, pages 270–280, Mar. 2003.
6. Toh C., "Associativity-Based Routing for Ad-Hoc Mobile Networks," Wireless Personal Comm., vol. 4, pp. 103-139, Nov. 1997.
7. Z. Zaidi and B. Mark, "A Mobility Tracking Model for Wireless Ad Hoc Networks," Proc. Wireless Comm. and Networking Conf.(WCNC), pp. 1790-1795, March 2003.
8. X. Lin, Y.K. Kwok, and V.K.N. Lau, "RICA: A Receiver-
9. Initiated Approach for Channel-Adaptive On-demand Routing in Ad Hoc Mobile Computing Networks," Proc. Int'l Conf. Distributed Computing Systems (ICDCS), pp. 84-91, July 2002.
10. B. Awerbuch, D. Holer, and H. Rubens, "High Throughput Route Selection in Multi-Rate Ad Hoc Wireless Networks," Proc. Conf. Wireless On-Demand Network Systems (WONS), pp. 251-269, March 2004.
11. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *IEEE Communications Magazine*, 40(8):102–114, Aug. 2002.
12. [2] C. L. Barrett, S. J. Eidenbenz, L. Kroc, M. Marathe, and J. P. Smith. Parametric probabilistic sensor network routing. In *Proceedings of the ACM International Conference on Wireless Sensor Networks and Applications (WSNA)*, pages 122–131, 2003.
13. [3] M. Burmester and T. V. Le. Secure multipath communication in mobile ad hoc networks. In *Proceedings of the International Conference on Information Technology: Coding and Computing*, pages 405–409, 2004.
14. [4] T. Claveirole, M. D. de Amorim, M. Abdalla, and Y. Viniotis. Securing wireless sensor networks against aggregator compromises.*IEEE Communications Magazine*, pages 134–141, Apr. 2008.
15. [5] D. B. Johnson, D. A. Maltz, and J. Broch. DSR: the dynamic source routing protocol for multihop wireless ad hoc networks. In C. E. Perkins, editor, *Ad Hoc Networking*, pages 139–172. Addison Wesley, 2001.
16. [6] P. C. Lee, V. Misra, and D. Rubenstein. Distributed algorithms for secure multipath routing. In *Proceedings of the IEEE INFOCOM Conference*, pages 1952–1963, Mar. 2005.
17. P. C. Lee, V. Misra, and D. Rubenstein. Distributed algorithms for secure multipath routing in attack-resistant networks. *IEEE/ACM Transactions on Networking*, 15(6):1490–1501, Dec. 2007.