MARS: Misbehavior Detection in Ad Hoc Networks

Li Zhao and José G. Delgado-Frias
School of Electrical Engineering and Computer Science
Washington State University
Pullman, WA 99164-2752, U.S.A.
{lzhao, jdelgado@eecs.wsu.edu}

***Abstract*—To detect misbehavior on data and mitigate adverse effects, we propose and evaluate a MultipAth Routing Single path transmission (MARS) scheme. The MARS combines multipath routing, single path data transmission, and end-to-end feedback mechanism together to provide more comprehensive protection against misbehavior from *individual or cooperating* misbehaving nodes. The MARS scheme and its enhancement E-MARS are evaluated by means of simulation under various adverse scenarios. The simulation results show that the MARS and E-MARS schemes provide better network performance and considerable protection to data transmission than some DSR-based transmission systems at the expense of moderate overhead. Compared to the DSR-based schemes, the proposed schemes deliver up to 45% more data with 20% misbehaving nodes under individual misbehavior, and up to 28% more data with 40% misbehaving nodes under colluded misbehavior.**

I. INTRODUCTION

An open mobile ad hoc network (MANET) can work effectively only if the different types of mobile nodes in it cooperate properly. Misbehaving nodes, including malicious nodes and selfish nodes, can disrupt the network operation and damage the communication within the network area. In order to minimize adverse effects of various types of misbehavior, the misbehaving nodes need to be detected and thus avoided by the system. Misbehavior detection and mitigation in MANETs is an important and critical research topic.

In the MANETs, different misbehaving nodes form misbehavior with different purposes. A selfish node may participate in the route discovery and maintenance processes and transmit control packets to benefit itself, but refuse to forward data packets for others in order to save its own energy. On the other hand, the malicious nodes need to participate in the route discovery and maintenance processes and transmit control packets normally to put themselves on utilized paths and get chance to manipulate (drop or change) transmitted data packets. In this paper, we focus on detecting and mitigating such misbehavior efficiently and accurately.

The traditional security mechanisms may not be fully applicable to a MANET due to its absence of infrastructure, consequent absence of authorization facilities, and distributed environment. It is difficult to make the mobile nodes establish trust relationship with each and every peer they are transiently associated with. This impedes providing cryptographic protection and authentication to all control and data traffic in the network. Moreover, even if this type of services were possible, the associated overhead and delay would pose a challenge in such a dynamic environment, and they cannot be effective against data dropping misbehavior. Thus, security schemes specified to the ad hoc environment are necessary.

There are many studies on detecting and mitigating misbehavior on data transmission in MANETs [2-7]. These studies are summarized in [8]. In this paper, we propose and enhance a **M**ultip**A**th **R**outing **S**ingle path transmission (MARS) scheme to mitigate adverse effects of misbehavor. It combines multipath routing and single path data transmission with end-to-end feedback mechanism. It is assumed that the required paths, which may not be free of misbehaving nodes, between end nodes have been discovered by routing protocols. The source selects two node-disjoint paths: one is used for data transmission; the other is for transmission information exchange. The destination detects misbehavior and notifies source through the feedback mechanism. The adverse effects are mitigated without restrictive assumptions on the network nodes' trust, without the use of intrusion detection schemes, and at the expense of moderate overhead only.

As the MARS employs single path data transmission, it is compared with Dynamic Source Routing (DSR) [1]-based secure and non-secure single path transmission systems under adverse environments. The simulation results show that the MARS provides better network performance and detects and mitigates various types of misbehavior on data at the expense of moderate overhead. The network remains efficient and effective even under very highly adverse environments.

This paper has been organized as follows. The misbehavior on data is discussed in Section II. In Section III, the proposed MARS scheme and its enhancement E-MARS are discussed in detail. In Section IV, the performance evaluation of the schemes through simulation experiments is presented. Some concluding remarks are provided in Section V.

II. MISBEHAVIOR ON DATA

The misbehaving nodes in an ad hoc network form different types of misbehavior out of different purposes. The types of misbehavior on data related to our work are discussed here.

A. Data Dropping

This is the denial of service (DoS) attack in which the selfish or malicious intermediate nodes refuse to forward data packets for other nodes in the network. Two adverse environments are examined in this paper. They represent the types of data dropping misbehavior formed by individual and cooperating misbehaving nodes respectively.

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2007 proceedings.

A1. Individual dropping: This is a relatively simple type of misbehavior. Due to different intentions, the misbehaving nodes drop all or a certain percent of the data packets they receive. Most schemes [2-6] detecting misbehavior on data have aimed to cope with this type of misbehavior.

A2. Colluded dropping: This is a widely-mentioned and sophisticated type of misbehavior formed by two cooperating malicious nodes. It is more furtive and harder to be detected and defended. It is assumed that two malicious intermediate nodes N1 and N2 are connected on a data transmission path. N1 forwards received data packets to N2, and N2 drops all or part of them. N1 tries to cover the data droppings at N2 by ignoring it and/or generating/forwarding faked acknowledgements in the system. As N1 would not report the misbehavior of N2 to the system, the overhearing schemes [2, 3] fail to detect such colluded misbehavior. Since N1 could forward faked 2ACK generated by N2 or generate faked 2ACK for N2, neither of the protocols proposed in [4, 5] could detect such fabricated packets and this colluded dropping. The schemes discussed in [6-7] can tackle such colluded misbehavior.

B. Data Modifying

The malicious nodes modify the received data packets during their transmission. The data modifying misbehavior is assumed to be formed individually by one malicious node along the data transmission path. The schemes in [4-5] cannot detect such type of misbehavior, while the schemes in [6-7] can effectively detect such misbehavior.

The MARS scheme discussed in this paper contains the mechanism to effectively detect and mitigate both the above mentioned data dropping and data modifying misbehavior.

III. The MARS Scheme

In this section, the MARS is presented. It is based on an early work presented in [11]. Many further developments and research, including timeout parameter, packet authentication, list update at destination, and detection of different types of misbehavior, are proposed and discussed in detail here.

A. Overview of the MARS Scheme

The MARS scheme tackles misbehavior through the use of two new types of control packets, termed INF and NTF. An INF packet, used to detect misbehavior, is sent from the source to the destination at the start of data transmission. A NTF packet, used to mitigate the adverse effects, is sent from the destination to the source when suspected misbehavior along data transmission path is detected.

In the MARS, the source keeps a Temp Route Pair List (TRPL) that contains pairs of node-disjoint paths that obtained from routing processes. The source gets a pair of paths, R1 and R2, from the TRPL before sending out data packets. To help the destination monitor the performance of R1, which is the shorter path of the pair used for data transmission, an INF packet is sent to R2 right after the first data packet has been sent to R1. Both the first data packet and the INF packet contain the information of this transmission.

To detect misbehavior, two lists called waiting list (WL) and confirmed list (CL), as shown in Fig. 1, are maintained at

Source ID (Waiting for Confirmation)	Timeout Value	R1 (Route1) R2 (Route2)	Data Information

(a) waiting list.

Source ID (Confirmed)	R1 (Route1) R2 (Route2)	Data Information

(b) confirmed list.

Fig. 1. Lists kept in destination for misbehavior detection.

the destination. Upon receiving a packet containing new transmission information from source, the destination puts the source ID, a timeout value τ, and the transmission information into the WL. A timer set to value of τ starts. If the destination receives a second packet containing matched transmission information from the desired path before the timeout expires, it admits that both paths work well currently. The source ID with the corresponding information is then moved into the CL.

After the source ID and corresponding information has been moved into the CL, the destination keeps a value S to record the number of received data packets during each observation time T. At the end of each observation time, the destination compares the statistic value S/T with the data rate value in the data information saved in the CL. When it detects the data dropping or data modifying misbehavior, the destination sends a NTF packet back to source through R2 and removes the source ID and corresponding items from the lists.

Upon receiving a NTF packet, the source removes this pair of paths from its TRPL and route cache. If it still has data to send, the source checks the TRPL for another pair of node-disjoint paths and sends an INF and data packet containing new transmission information. The source initiates a route request procedure if no node-disjoint paths are available in the TRPL. The destination removes the corresponding items from the lists when it receives a RREQ from source, and updates the lists when it receives packets containing new information.

B. New Control Packets

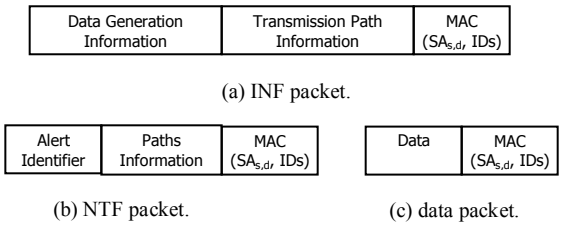
An INF packet contains information of the corresponding transmission: (a) data generation information such as data generation rates, data packet size, and expected data amount; (b) data transmission path information, including the path length and nodes along the path. An INF packet can also carry a randomly generated key to authenticate the data packets of the corresponding transmission batch.

A NTF packet contains an alert identifier and information of path pair, including lengths of paths and nodes along paths.

C. Packet Authentication

It is assumed that a security association ($SA_{s,d}$), such as a symmetric shared key, between the source and the destination exists in the MARS. Since two nodes choose to employ a secure communication scheme, their ability to authenticate each other is indispensable.

Each of the data and control packets in the system carries a message authentication code (MAC) calculated from the source and destination IDs and the $SA_{s,d}$. As a result, the end nodes can verify the integrity and the authenticity of these packets, whose structures are shown in Fig. 2.



(a) INF packet.

(b) NTF packet.

(c) data packet.

Fig. 2. Structure of different packets for security transmission.

D. Timeout at Destination, τ

The parameter timeout τ is used to set up a timer for items in the waiting list at the destination. If the timer expires before the matched information is received, the destination claims detecting misbehavior on data, and a NTF packet is sent back to the source. It is clear that false alarms may be triggered if τ is too small. On the other hand, if τ is too large, the destination will be too slow in detecting misbehavior, and this may cause relatively big delay in the network. Thus, an appropriate value of τ is important for the performance of the MARS scheme.

The timeout value τ is related to the difference between the lengths of the selected node-disjoint paths and the current network traffic. It should satisfy

$$\tau > \max\left(\frac{T_1}{l}, \frac{T_2}{l'}\right)\left|l - l'\right| \quad (1)$$

where l and l' are the lengths of the paths, and T_1 and T_2 are the times that take a packet to transmit through a path with length l and l' respectively.

E. List Update at Destination

If new transmission information from a source is received while the previous information of the same source is waiting for confirmation, the destination updates the corresponding item at the WL. If new transmission information is received after the previous information of the source has been confirmed, the destination removes the corresponding item from the confirmed list and add a new item in the waiting list. The destination removes the corresponding items from the WL or CL when it receives a new RREQ from a source.

F. Misbehavior Detection at Destination

The MARS scheme can efficiently detect the types of misbehavior on data discussed in Section III. Here, the misbehaving nodes are assumed to manipulate the transmitted data but forward the control packets.

If all data packets are dropped by misbehaving nodes along R1 individually or collaboratively, the destination would not receive the data packet with matched transmission information within the timeout limit. The misbehavior is then detected.

If the data packets are partly discarded to a certain extent, the difference between the statistic value S/T, which is obtained after an observation period T, and the data rate value, which is delivered by INF packet and saved in the CL, would exceed a specified limitation. Hence, from the information saved in the CL, such misbehavior would still be detected.

If the data packets are modified during transmission, the destination would detect this through calculating the message authentication code (MAC) in the data packets.

Whenever the misbehavior is detected, the source ID and the corresponding transmission information are removed from the lists. A NTF packet is sent back to the source through R2.

G. Multipath Routing Algorithm

The MARS can operate with any underlying routing protocols [1, 6, 9] that can obtain two node-disjoint paths between the source and destination. A more efficient multipath routing algorithm can help the MARS achieve larger benefits.

The security of routing discovery is provided by the security mechanism integrated in the routing protocols. This is not the focus of this paper. In this study, we use a DSR-based multipath routing algorithm, which employs a heuristic redirection method described in [9]. Two node-disjoint paths with the minimum sum of hops are selected by the source. Please refer to [9] for details of the routing algorithm.

H. An Enhancement of MARS, E-MARS

The delay of a data packet in the network is composed of transmission time along the path and waiting time at the source and intermediate nodes. In the MARS scheme, the time that data packets stay in source buffer before the establishment of node-disjoint paths contributes partly to its end-to-end delay. An enhancement, E-MARS, to the MARS is presented here to decrease this buffering time.

In E-MARS, the source transmits the buffered data packets through the first established path. A new generated data packet is transmitted through the shortest cached path when the node-disjoint paths are not available. No transmission information is piggybacked in these data packets and no INF packet is transmitted in the above two cases. The data transmission follows the MARS once two node-disjoint paths are available.

The E-MARS could decrease the end-to-end delay in the network. The cost is that the source may not be aware of misbehavior on transmitted data in time in some cases.

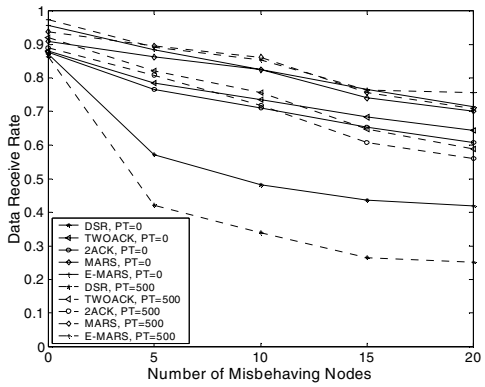
I. Features of the Schemes

The MARS and E-MARS schemes require a security association only between the source and destination. None of the end nodes needs to be securely associated with any of the remaining nodes in the network. Thus, unlike the schemes in [2-5], the MARS and E-MARS do not require cryptographic operations and authentications at intermediate nodes.

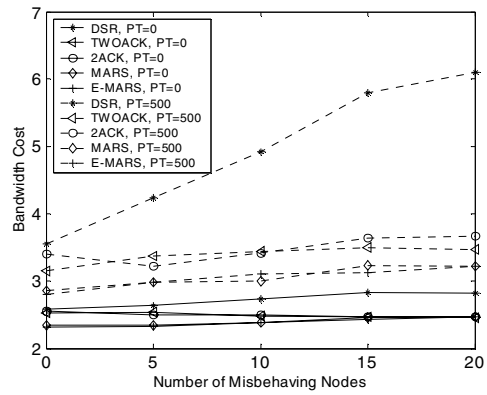
As there is a reliable end-to-end feedback channel between two end nodes, any misbehavior detected by the destination can be reported back to the source promptly. The schemes can detect and mitigate various types of misbehavior on transmitted data formed by individual or cooperating nodes.

Compared with the schemes in [2-5], the MARS and E-MARS can solve the problem of colluded misbehavior along one path. Different from schemes in [6-7], these proposed schemes employ single path data transmission. Different from other misbehavior detection schemes [2-5], the MARS and E-MARS puts the misbehavior detection at the destination end. Furthermore, different from the acknowledgement packets in some schemes [4, 5], the NTF packet in the MARS is sent out only when the destination detects misbehavior on data to minimize the control packet overhead.

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2007 proceedings.

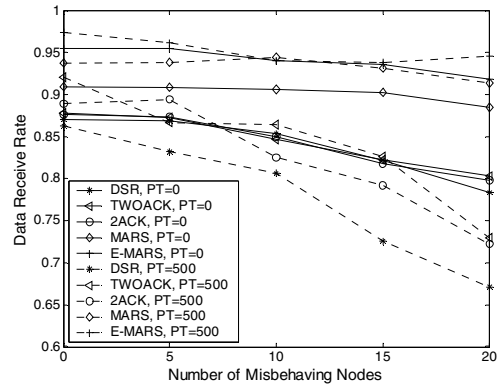


(a) Data receive rate.

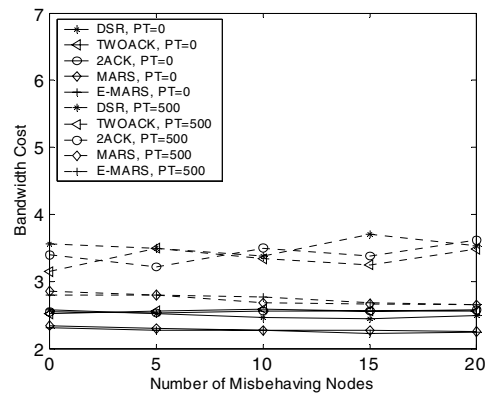


(b) Bandwidth cost for data.

Fig. 3. Individual dropping.



(a) Data receive rate.



(b) Bandwidth cost for data.

Fig. 4. Colluded dropping.

IV. PERFORMANCE EVALUATION

To evaluate the performance of the MARS and E-MARS, the two types of dropping misbehavior discussed in Section II are considered. Since both MARS and E-MARS implement single path transmission, they are compared to the DSR-based 2ACK [5] and TWOACK [4] schemes and original DSR system [1] by means of simulation. Similar to the E-MARS being an enhancement of the MARS, the 2ACK is a modification of the TWOACK. It is assumed that the correctness of the discovered connectivity is guaranteed in all cases.

A. Simulation Methodology

In the simulations, we use the GloMoSim [11] library-based simulator. 50 nodes, each with a radio power range of 376 meters, are placed randomly within a 1200-meter×1200-meter area. The channel capacity is 2Mbps. The timeout value τ at destination set to 1.0 and 8.0 seconds. The IEEE 802.11 DCF is used as the MAC layer protocol. Each node is assumed to move independently in the random waypoint model with the same average speed. The minimum and maximum speeds of node movement are 0 and 20m/s. Two node pause times, 0 and 500 seconds that represent fast and slow node mobility, are considered. The sources and destinations of 10 CBR data sessions are chosen uniformly. The data packets of size 128 bytes are generated with interval 0.5 second. The percentage of misbehaving nodes in the network is varied from 0 to 40%. The misbehaving nodes are assumed to drop all received data packets. In the 2ACK, the τ = 0.15 second, R_{ack} = 0.20, and R_{mis}=0.85. In the TWOACK, τ = 0.15 second, the threshold of maximum error is 5. Each simulation runs 10 sessions.

B. Performance Metrics

The performance metrics used to evaluate the MARS and E-MARS schemes are:

B1. Data Receive Rate (DRR): the ratio of the number of data packets received at the destinations and the number of data packets sent by the sources;

B2. Bandwidth Cost for Data (BCD): the ratio of the number of data packets transmitted by all nodes normalized by the number of data packets received at the destinations;

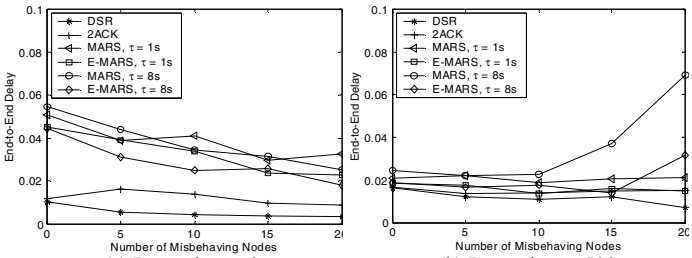
B3. Average End-to-end Delay (AED): the end-to-end delay averaged over all surviving data packets for each source/destination pair.

C. Simulation Results

The benefit from implementing multipath routing and fewer control packets mechanism is shown in Fig. 3 and Fig. 4, in which the timeout value τ is 1.0 second. When all nodes are benign, the MARS and E-MARS have higher DRR and lower BCD than the 2ACK, TWOACK, and DSR systems.

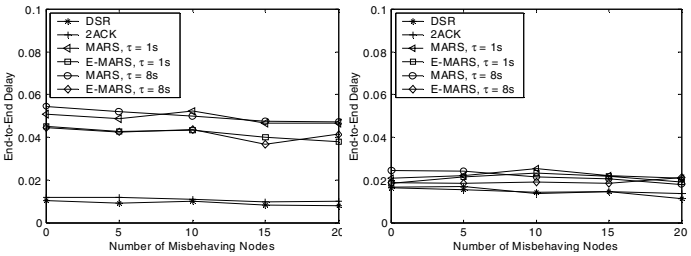
As shown in Fig. 3(a) and Fig. 4(a), the MARS and E-MARS provide more protection to data communication under both adverse cases. The DRR decreases as the number of misbehaving node in the network increases. With pause time 500 seconds and 20% misbehaving nodes, the DRR of DSR

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2007 proceedings.



(a) Pause time = 0s. (b) Pause time = 500s.

Fig. 5. Individual dropping.



(a) Pause time = 0s. (b) Pause time = 500s.

Fig. 6. Colluded dropping.

decreases more than 50% under individual dropping and 8% under colluded dropping. Under the same conditions, the DRRs of the MARS and E-MARS decrease only around 7% and 1% respectively. The MARS and E-MARS deliver about 90% data packets while DSR delivers only 34%. Even with 40% misbehaving nodes, the DRRs of MARS and E-MARS are about 50% higher under individual dropping and about 28% higher under colluded dropping than those of DSR. The MARS and E-MARS provide similar protection for data transmission with the TWOACK and 2CK under individual dropping. They outperform the TWOACK and 2ACK due to fewer control packets. As the 2ACK and TWOACK have no mechanism to detect colluded dropping, their DRRs decrease just like those of DSR with the increase of misbehaving nodes under such misbehavior. On the contrary, the DRRs of the MARS and E-MARS are almost constant regardless of the percentage of misbehaving nodes under colluded misbehavior.

Fig. 3(b) and Fig. 4(b) indicate that the DSR, 2ACK, and TWOACK have higher BCD compared to the MARS and E-MARS. With the decrease of node mobility, the bandwidth cost for data of DSR increases dramatically.

As two node-disjoint paths are needed to start the data transmission and the selected path may not be the shortest one in source cache, the AEDs of our MARS and E-MARS are higher than those of the DSR and 2ACK, as shown in Fig. 5 and Fig. 6. Since the MARS needs two node-disjoint paths before the start of data transmission, it has the highest AEDs. The E-MARS has lower AEDs as expected. This is the moderate overhead due to multipath routing. Lower node mobility corresponds to lower route refresh frequency and less buffering time of data packets in the source. The delays of the MARS and E-MARS are quite close to those of DSR and 2ACK when pause time is 500 seconds.

To investigate the impact of timeout parameter on network performance, two values of τ, 1.0 second and 8.0 seconds, are tested under various adverse environments. As shown in Fig. 5 and Fig. 6, different values of τ make different AEDs of the schemes mainly when there is a high percentage (> 30%) of misbehaving nodes in a slow mobile network under individual dropping. The variations of DRR and BCD of network for different values of τ are ignorable and thus not shown here.

The simulation results show that the MARS and E-MARS schemes are more suitable for slow mobile ad hoc networks. In such a network, they provide significant protection to data transmission with neglectable overhead.

Due to the integrated authentication mechanism, the MARS and E-MARS can also detect the data modifying misbehavior efficiently. As this is not the most significant function of these schemes focused in this paper, the simulation results under such adverse environments are not presented here.

V. Conclusions

In this paper, we have presented a novel scheme MARS and its enhancement E-MARS to detect misbehavior and mitigate adverse effects in ad hoc networks. They have been compared with the 2ACK and TWACK secure schemes and DSR transmission systems under various adverse environments by means of simulation. Our study shows that the proposed schemes have the following features:

- *Effectiveness*. The MARS and E-MARS effectively detect individual or colluded misbehavior in ad hoc networks.
- *Scalability.* The MARS can be modified to provide further data protection and better network performance. The E-MARS discussed here has convincingly proven this. A reputation system can also be introduced into these schemes.

Although sybil attack [12], in which a single node presents multiple identities to other nodes, can reduce the effectiveness of multipath routing and make these schemes fail to work, our schemes in combination with countermeasures, such as radio resource testing, position verification and random key pre-distribution, will be able to defend from sybil attack.

References

[1] J. Broch, D. Johnson, and D. Maltz, "The dynamic source routing protocol for mobile ad hoc networks," *http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-04.txt*, Nov. 2000, IETF Internet Draft.

[2] S. Marti, T.J.Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *Proc. MobiCom 2000*.

[3] K. Paul and D. Westhoff, "Context Aware Detection of Selfish Nodes in DSR based Ad-hoc Networks," *Proc. GlobeCom 2002*.

[4] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: preventing selfish in mobile ad hoc networks," *Proc. WCNC'05,* 2005.

[5] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgement-based approach for the detection of routing misbehavior in MANETs," *IEEE Tran. Mobile Computing*, 2006.

[6] W. Lou, W. Liu, and Y. Fang, "SPREAD: enhancing data confidentiality in mobile ad hoc networks," *IEEE INFOCOM 2004,* pp. 2404 – 2413.

[7] K. Stewart, T. Haniotakis, and S. Tragoudas, "A security protocol for sensor networks," *Proc. IEEE GlobeCom 2005*.

[8] L. Zhao, "Enhance communication security in wireless ad hoc networks through multipath routing", Ph.D. Dissertation, Washington State University, 2007.

[9] K. Wu and J. Harms, "Performance study of a multi-path routing method for wireless mobile ad hoc networks," *Proc. MASCOTS' 01*, pp. 99-107.

[10] L. Zhao and J. G. Delgado-Frias, "Multipath Routing Based Secure Data Transmission in Ad Hoc Networks," *Proc. WiMob'06*, pp. 17-23.

[11] X. Zeng, R. Bagrodia, and M. Gerla, "GloMoSim: a library for parallel simulation of large-scale wireless networks," *Proc.PADS'98*.

[12] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis and defenses," *Proc. IPSN' 04*, pp. 259-268.

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2007 proceedings.