Multipath Routing Based Secure Data Transmission 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, USA
{lzhao, jdelgado@eecs.wsu.edu}

***Abstract*—The specific characteristics of Mobile Ad Hoc Networks (MANETs) make cooperation among all nodes and secure transmission important issues in its research. Misbehaving nodes with different intentions and capabilities would conduct various types of misbehavior in the networks. In this paper, we present and evaluate a scheme, in which multipath routing combined with feedback mechanism are used to tackle misbehaviors on data delivery formed by *one or more* misbehaving nodes in an ad hoc network. Data and control packets are transmitted through two node-disjoint paths. The source is notified of suspected misconduct of intermediate nodes through feedback mechanism. A simple derivation of this scheme is also discussed. The proposed scheme and the derivation are compared with the single path routing protocol DSR by means of simulation implemented at normal and adverse scenarios. The simulation results show that the proposed scheme and the derivation provide considerable protection in ad hoc networks at the expense of moderate overhead introduced by multipath routing. In a network with up to 40% misbehaving nodes, the proposed scheme and the derivation result in around 17% in data receive rate over the single path DSR.**

***Index Terms*—security, data transmission, multipath routing, ad hoc networks**

I. Introduction

A mobile ad hoc network (MANET) is a collection of wireless mobile nodes that communicate peer-to-peer in a self-organized manner without fixed network infrastructure or any centralized administration. The transmission range of each node is limited. Thus, each node needs to perform routing/data delivery, forwarding control/data packets for others. With dynamic topology, distributed cooperation and constrained capability, an ad hoc network can work effectively only if the participating nodes cooperate in a proper way. These characteristics make collaboration among all nodes and secure data transmission important and, in many cases, critical issues in the research of ad hoc networks.

There are two types of misbehaving nodes in an ad hoc network. Malicious nodes, also called attackers, are controlled by adversaries. They intrude the network with intention to cause harm. They are capable of discarding or altering control and data packets, preventing route discovery between two nodes, make data packets unable to arrive at their destination while consuming energy and available bandwidth of the network, etc [4], [15]. Selfish nodes are part of the ad hoc network. They use the network for their own communication, but refuse to spend their precious power for operations that do not directly benefit themselves. They can drop data packets or refuse to forward routing control packets for other nodes. Although they are not intended to damage the network, their behavior corrupts the performance and influents the operation of the whole network.

Our focus in this paper is on detecting the misbehaving nodes that participate in the route discovery and maintenance processes but refuse to forward data packets to the next node along path. They can misbehave in two forms. *Dropping data* is formed by one individual misbehaving node on the data transmission path. *Colluded dropping* is formed by two colluding misbehaving nodes connected on the data transmission path. The first misbehaving node forwards the data packets it receives to the next one. The next misbehaving node drops the data packet instead of forwarding it to its next node along the path. This kind of misbehavior is more dangerous and difficult to be detected and defended.

In this paper, we present and evaluate an end-to-end scheme aimed at safeguarding data transmission from the above node misbehavior in ad hoc networks using multipath routing combined with feedback mechanism. The source gets two node-disjoint paths by implementing multipath routing algorithms. Data and control packets are sent through these paths to the destination. Single path data transmission is implemented. The destination notifies the source of suspected misconducts in the intermediate nodes along the paths through feedback mechanism. A derivation of this scheme to reduce data packet delay is also presented. Their performance is compared with that of the single path routing DSR and evaluated under normal case and at scenarios when individual and cooperating misbehaving nodes conduct misbehavior on the transmitted data packets. The simulation results show that the proposed scheme and the derivation guarantee the data receive rate of the network at various cases and remains efficient and effective even in highly adverse environments.

1-4244-0495-9/06/$20.00 ©2006 IEEE

The rest of this paper is organized as follows. In Section II, a summary of related work on mitigating routing and data transmission misbehavior and multipath security protection in ad hoc networks is presented. In Section III, the proposed scheme and its derivation are described in detail. Section IV presents the simulation model and the performance evaluation results. Some concluding remarks are given in Section V.

II. Related Work

Security issues in ad hoc networks have been well enumerated in the literature [4], [15], and there are many proposed protection protocols [1], [4], [7], [10]. In this section, we provide a brief description of previous work on mitigating the misbehavior discussed in this paper.

A. Single Path Security Schemes

Various mechanisms to prevent misbehavior on routing and data transmission in ad hoc networks have been proposed. To detect and mitigate the routing misbehaviors in ad hoc networks, Marti et al. [8] propose a reputation-based scheme composed of two modules called watchdog and pathrater. The watchdog overhears the medium to check whether the next-hop node faithfully forwards the packet or not and accordingly decide whether to clear a data packet in the buffer or not. Based on the information the watchdog collects, the pathrater rates each path and chooses the path with the fewest misbehaving nodes. Two network-layer acknowledgement-based schemes, TWOACK and its derivation S-TWOACK, are proposed in [1] to detect the selfish nodes that refuse to forward data packets for others, and alleviate the problem using a reputation-based system. A node acknowledges the receipt of a data packet from its previous node by sending back a two-hop TWOACK packet along the active source route. If the sender/forwarder of a data packet does not receive a TWOACK corresponding to a particular data packet it has sent out within a time limit, the next-hop's forwarding link is claimed to be misbehaving and the forwarding route is broken. Based on this claim, the routing protocol avoids the accused link in all future routes. The S-TWOACK scheme is an enhancement of TWOACK, aimed at reducing the routing overhead caused by excessive number of TWOACK packets.

These single path security schemes are relatively simple. They can detect data dropping conducted by one individual misbehaving node. However, they fail to detect fabricated or colluded misbehavior.

B. Multipath Security Schemes

Several protocols using multiple paths between source and destination to provide secure data transmission in wireless ad hoc networks have been studied. Zhou and Haas [15] initially proposed using multiple routes between nodes, just like what diversity coding did, to defend routing against denial-of-service (DOS) attacks.

Recently, several studies have been conducted on providing protection on data transmission by using multiple node-disjoint paths between the source and the destination [7], [10]. Papadimitratos and Haas [10] present and evaluate the Secure Message Transmission (SMT) protocol, which fights against malicious behavior of intermediate nodes on data transmission in the network. With SMT, when the source has a set of node-disjoint paths (APS) to a specific destination, it divides each outgoing message into a number of pieces using some message dispersal scheme, which adds limited redundancy to the transmitted data, and sends them into different routes in APS. At the destination, the received pieces are validated and the successfully received ones are acknowledged to the source through a dispersed and cryptographically protected feedback mechanism. A dispersed message is successfully reconstructed if enough pieces are received. The missing packets of an unreconstructed dispersed message will be retransmitted by the source for a limited times. While sending data packets and receiving acknowledgements to and from the paths, the source rates the paths in APS and discards invalid ones.

Lou et al. [7] propose and investigate a scheme called SPREAD, which provides further protection to the existed data confidentiality service in an ad hoc network using multi-path routing. It aims to protect secret message from being compromised. A secret message is transformed into multiple shares using the threshold secret sharing algorithm, which also introduces some redundancy into the system. The shares are delivered via multiple node-disjoint paths to the destination. At the destination, the secret message is reconstructed if sufficient numbers of shares are received. As the shares are delivered through multiple node-disjoint paths, the secret message as a whole is not compromised even if a small number of shares are compromised. The attack considered in [7] is *colluded attack*, in which there is at least one compromised node on each of the selected paths, and the enemy can control all of these compromised nodes. The data transmission mechanisms at SMT and SPREAD both are basically the combination of multipath routing and multiple description coding (MDC).

Although the use of multiple paths in an ad hoc network could diminish the effect of unreliable wireless links and misbehavior of individual and colluded intermediate nodes to make transmitted messages safer, the interference between different paths at source and destination and the interactions between the MAC layer protocol and the network-layer data transmission impact negatively on the performance of multipath data transmission system. Moreover, the selected node-disjoint routes between the source and the destination are generally not the ones with the shortest hop length.

In the proposed scheme, one single path, rather than the multiple diversity mechanism, is used for data transmission. Thus, there is no message disperse procedure needed in the source and no message reconstruction procedure in the destination. There is no redundancy introduced into the network traffic, and no interference of multiple paths at the

source and destination area. These are its main differences from the protocols proposed in [7], and [10].

III. The Proposed Schemes

In this section, the proposed schemes are presented. First, we describe the multipath routing algorithms used in our scheme. Later, we explain the data transmission and information exchange mechanism in the scheme and a derivation of it.

A. Multipath Routing Algorithms

Because of the node mobility and topology changing, multipath routing in ad hoc networks presents great challenge. In some single path routing protocols, such as the Dynamic Source Routing (DSR) [2] and the Temporally Ordered Routing Algorithm (TORA) [11], multiple paths can be found and used as a backup in data transmission. There are some algorithms focusing on searching multiple paths in ad hoc networks. A diversity injection method is proposed in [12] to find more node-disjoint paths than DSR can. The Split Multipath Routing (SMR) [6] is proposed to find the maximally node-disjoint paths in ad hoc networks. An on-demand method proposed in [13] is more efficient in searching multiple node-disjoint paths. A maximal node-disjoint path finding algorithm described in [7].

The proposed scheme can operate with any underlying multipath routing protocol. A more efficient routing protocol can certainly make the scheme exhibit its benefits better. Two algorithms are used here to obtain multiple paths for the proposed scheme. One is a modified version of the optimized DSR [2], in which a source implementing DSR is capable of getting multiple paths from its route cache. The other is the on-demand multipath routing algorithm proposed in [13]. It is based on DSR with four main modifications:

--First, the later-received RREQ in the intermediate nodes are cached instead of dropped.

--Second, only the destination sends RREP packets back to the source.

--Third, the RREP includes a label *isRedirection* to indicate whether the RREP packet should be redirected when traversing back to the source. If the path included in the received RREQ packet is node-disjoint with all paths included in its cached RREQ, the destination sends a RREP packet to the source using the reverse path with *isRedirection* be FALSE. Otherwise, the *isRedirection* in the RREP sent back to the source is set to be TRUE.

--Forth, when an intermediate node receives a RREP with *isRedirection* be FALSE, it forwards the RREP to the next node. Or else, it checks if there is a path node-disjoint with the remaining hops included in the RREP packet in its cached RREQ. If so, it redirects the RREP following this cached path and set the *isRedirection* in the RREP to FALSE.

B. Data Transmission and Information Exchange

The principle of the proposed scheme is to guarantee data packets reach destination. The security solution is provided at IP layer. Two node-disjoint paths are needed between source and destination, but only one of them is used to transmit data. Two types of control packet are introduced into the system. CONNECT is sent from source to destination after the two paths are selected, and NOTIFY is sent from destination to source when suspected misbehavior along data transmission path is detected. A time parameter, termed *timeout*, is set at destination. It is the allowable time between two packets containing matched connect information arriving destination.

When the source is ready to send data and cannot find two node-disjoint paths to the destination in its cache, it launches the multipath route discovery procedure. The two node-disjoint paths the source gets from the route discovery procedure are used for different purposes. The shorter path, called Route1, is the primary path for data transmission. The longer path, called Route2, provides channel for control information exchange.

Once the source selects these paths, it notifies the destination of their route information, which contains the path lengths, nodes along each path and whether it is the data transmission path. The information about Route2 is piggybacked in the first data packet and sent through the primary path (Route1), while the information about Route1 is sent right after the first data packet into Route2 in a CONNECT packet. After having successfully received the matched route information from two paths, the destination establishes a reliable feedback channel to notify the source of misbehavior on the transmitted data packets. If necessary, this feedback channel also can be used by the two ending nodes to exchange other information, such as cryptography or authorization information, to make the destination not be cheated by the malicious nodes, which may modify the transmitted data packets.

Two lists, given in Fig. 1, are kept in the destination for misbehavior detection. The left list contains the source ID, from which two packets containing matched information have been received from two node-disjoint paths within the *timeout,* and the corresponding path information. Both paths from these sources to the destination are validated working well. The destination keeps track of the received data packets from them. The right list contains the source ID from which only one packet containing path information has been received within the past time τ_w, which is smaller than the *timeout*, and the corresponding path information. As the problem concerned

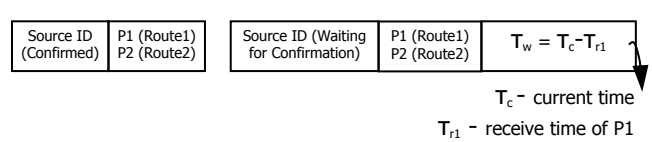

Fig. 1. Two lists kept in destination for misbehavior detection.

in this paper is misbehaving nodes dropping data packets, the received packet is CONNECT. If the waiting time τ_w becomes larger than *timeout* and the destination still could not receive the data packet containing matched path information, a data or CONNECT packet containing new paths information, or a new route request packet indicating broken primary path from the source, the destination determines that an intermediate node along the data transmission path drops data packets. Thus, it sends a NOTIFY packet to the source through the valid path from which the CONNECT packet is received.

If one of the paths is broken due to link failure, the source would receive a route error packet. If the primary path suffers misbehavior of the intermediate nodes, the source would receive a NOTIFY packet from the destination. After having received one of these two alarms, the source checks its cache to see if another two node-disjoint paths to destination exist in it cache if it still has data to send. If there are such paths, the source sends new route information and data packets through the new paths to the destination. Or else, the source initiates a multipath route request procedure for new paths.

To diminish their influence of the two new control packets to the network traffic, the route information transmitted along the primary path is piggybacked on a data packet, and the NOTIFY packet is only needed when the intermediate nodes refuse to forward data packets and the destination detects.

C. Derivation to Reduce Delay

In the scheme described above, when the source does not have two node-disjoint routes to the destination, its generated data packets have to be queued in the buffer. The queued data packets can only be sent after the source gets such two paths. As the delay of a data packet is composed of transmission time along the path and waiting time in buffer, the scheme increases the end-to-end delay in network. Therefore, we further propose a very simple derivation of the scheme to reduce the packet delay by decreasing the data packet waiting time in buffer. In the derivation, instead of sending a data packet only after having got two node-disjoint paths, the source sends the buffered data packets once it receives a route reply. That is the source sends buffered data packets through its first route to the destination.

Although the derivation is expected to reduce the end-to-end data packet delay in the network, it comes with a cost that the source may not be notified in time of data dropping along the first route.

D. Features of the Scheme

As the scheme builds an end-to-end feedback channel from the destination to source, any misbehavior causing a certain number of data packets losing during the proceed of transmission can be informed to the source. The source then can switch data transmission to other paths. Thus, the proposed scheme can detect and mitigate various types of misbehavior in ad hoc network, including those conducted by two or more cooperating misbehaving nodes.

However, the proposed scheme fails if the NOTIFY packet is lost during its transmission. And the routing overhead in system increases because of implemented multipath routing.

E. Comparison with COPAS

The proposed scheme has similar mechanism with COPAS presented in [3]. COPAS is proposed to tackle the capture problem on TCP over multihop ad hoc networks. It uses disjoint forward and reverse paths in order to minimize the conflicts of TCP data and ACK packets, and employs a dynamic contention-balancing scheme to minimize the likelihood of capture. There are three main differences between the proposed scheme and COPAS. First, the NOTIFY packets in the proposed scheme are different from the ACK packets in COPAS. In COPAS, the ACK packets at TCP layer are used for the purpose of flow-control and sent to acknowledge the source of data receiving. The NOTIFY packets in the proposed scheme are only sent to source when misbehavior in the intermediate nodes along the primary path is detected. Second, the proposed scheme is a network-layer protocol while COPAS is a transport-layer protocol. There is no disconnection process needed in the proposed scheme. Third, the destination selects those two paths in COPAS while the source selects those two paths in the proposed scheme.

In this section, we will look into how the proposed scheme defends against various misbehaviors on data transmission, and evaluate its performance under benefit and adverse environments by means of simulations.

IV. Performance Evaluation

A. Simulation Environment

We use the GloMoSim [14] library-based simulator to study the performance of the proposed scheme. The multipath routing protocols used are the on-demand multipath routing algorithm proposed in [13] and a modified version of the optimized DSR [2]. In the simulation, 100 mobile nodes are placed randomly within a 1200-meter×1200-meter area. Each run executes 600 seconds of simulation time. Each node has a radio power range of 627 meters. The channel capacity is 2Mbps. A free space propagation model with a threshold cutoff is used as the channel model. Capture effects are taken into account in the radio mode. The IEEE 802.11 Distributed Coordination Function (DCF) is used as the MAC layer protocol. Each node is assumed to moves independently in the random waypoint model with the same average speed. The sources and destinations are chosen randomly with uniform probabilities. The minimum and the maximum speed of the node movement are 0m/s and 20m/s, and the pause time is varied from 0 second to 600 seconds. There are 40 CBR data sessions. The interval time to send packets is 0.5 second. The size of all data packets is set to 512 bytes. The simulation parameters are summarized in Table 1.

TABLE 1.
COMMON SIMULATION PARAMETERS (SIMULATION AREA AND TIME VARIED)

Number of nodes	100
Transmission range	378 meters
Simulation area	1200-meter × 1200-meter
Simulation time	600 s
Packet size	512 bytes
Channel capacity	2Mbps
Number of CBR sessions	40
Packets sent interval	0.5 second
Minimum and maximum pause time	0m/s, 20m/s
Pause time (s)	0, 100, 200, 300, 400, 500, 600

B. Performance Metrics

The performance metrics used to evaluate the efficiency of proposed scheme under normal case are: packet delivery rate, average end-to-end delay, and bandwidth cost for data. *Packet delivery rate* is the total number of packets all nodes received normalized by the total number of packets they sent. *Average end-to-end delay* is the end-to-end delay averaged over all surviving data packets for each source/destination pair. *Bandwidth cost for data* is the total number of data packets all nodes transmitted normalized by the total number of data packets they received.

As what mainly concerned under adverse environment is the effect of misbehavior on data transmission in the network, the performance metrics evaluated is the data receive rate, which is the total number of data packets all nodes received normalized by the total number of data packets they sent.

C. Simulation Results

As mentioned earlier, we have investigated the performance of the proposed scheme under normal and adverse environments.

1) Under Normal Case: the single path DSR and the proposed scheme based on modified optimized DSR, the proposed scheme and the derivation based on the on-demand multipath routing algorithm [13] are compared. Fig. 2 shows the packet delivery rate of the proposed scheme on both multipath routing protocols and the derivation are less than that of the single path DSR, and the packet delivery rates of the proposed scheme based on two multipath routing algorithms and the derivation are very close to each other. Fig. 3 shows that the delay of the single path DSR is the smallest, and the delays of the proposed scheme and the derivation based on the on-demand multipath algorithm are medium, while that of the derivation is smaller than that of the proposed scheme by about 1 second. Fig. 4 shows that the bandwidth cost for data of single path DSR and those of the proposed scheme and the derivation based on on-demand multipath routing algorithm are almost the same, and that of proposed scheme based on optimized DSR is higher by 20% - 30% over the others.

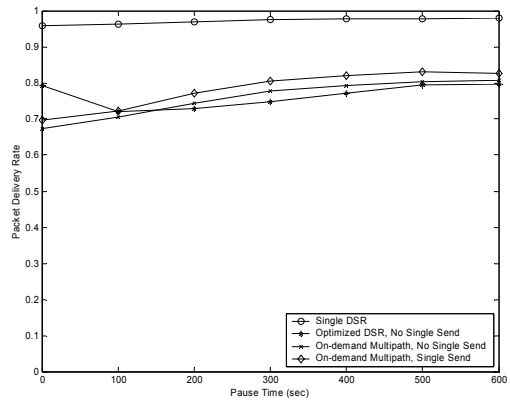

Fig. 2. Packet Delivery Rate.

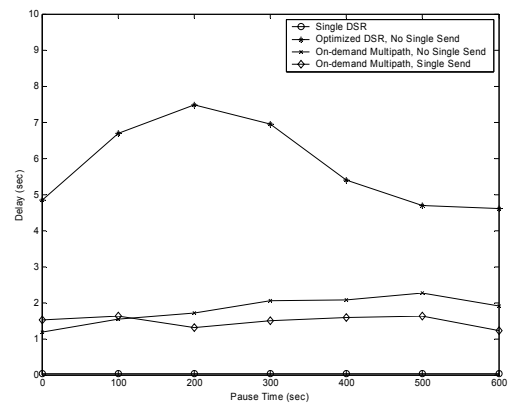

Fig. 3. Average End-to-End Delay.

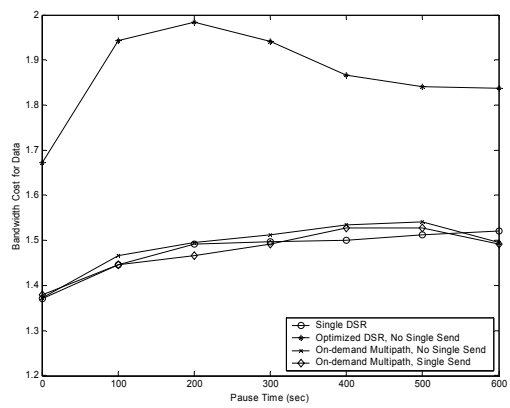

Fig. 4. Bandwidth cost for data.

Due to the requirement of two node-disjoint routes, the chosen route to transmit data packet may not be the shortest one in the route cache. This in turn increases the route searching packets in the network, the collision during data transmission, and the data packets waiting time in source buffer before being sent out. The derivation using first single path data transmission can reduce the data buffer time and thus reduce the end-to-end delay in the network. The comparison of network performance based on these two multipath algorithms indicates that a more efficient multipath

algorithm can yield a better performance of the proposed scheme. Hence, the proposed scheme based on the on-demand multipath routing algorithm is chosen to compare with the single path DSR under the following adverse environments.

2) Dropping Data: An individual misbehaving node along the data transmission path drops all received data packets instead of forwarding them. Fig. 5 shows the data receive rate in network suffering different percentage of dropping data misbehaving nodes. The percentage of misbehaving nodes in the network is varied from 0 to 40%. Two different node pause times are considered. With the increase of misbehaving nodes in network, the data receive rate for the single DSR decreases dramatically while those for the proposed scheme and the derivation are affected in a much lesser extent. For example, when 40% of nodes are misbehaving in the network, the data received rate of single routing path decreases around 29% while that of the proposed multi-path scheme decreases only around 9%. Thus, although the data receive rates of the proposed scheme and the derivation are less than that of the single path DSR when all nodes are well-behaved, they exceed that of the single path DSR when there are less than 10% misbehaving nodes in the network. The derivation can provide better overall performance than the proposed scheme.

When more misbehaving nodes exist in the network, the selected paths would more likely to include such nodes and the transmitted data would more likely be dropped during transmission. In the single path DSR, the source is not aware of the data dropping during transmission. Thus, it would continue sending out data packets until it receives a route error packet indicating the route breakage because of node mobility. So, the data receive rate decreases dramatically. In the proposed scheme, the source would be notified of the data dropping in time by the destination, and then switch the data transmission to other paths. Thus, the data receive rate can be guaranteed. And as the derivation transmits the buffered data packets through the shortest path to the destination, it achieves higher data receive rate than the original proposed scheme.

3) Colluded Dropping: If the misbehaving nodes in an ad hoc network cooperate with each other as a group, they can conduct the misbehavior in a way that the schemes proposed in [1] and [3] cannot detect. A simple cooperation way could be that they try to be connected with each other on a path. For example, during the route discovery process, after receiving a route request packet, instead of broadcasting the request to all its neighbors, a misbehaving node could repackage the request packet to make it only for its misbehaving neighbors and make no route involving normal nodes within its range area. Once a path on which two or more misbehaving nodes connected is selected for data transmission, the first misbehaving node forwards data packets to the next one. The next misbehaving node drops the packets. This colluded dropping is more furtive and harder to be detected and defended. It could be formed only on path with length equal to or larger than 3. To get long paths in the simulation of colluded dropping, some simulation parameters, showed in Table 2, are changed.

TABLE 2. NEW PARAMETERS FOR COLLUDED DROPPING SIMULATION.

Parameters	Value
Simulation area	1800-meter × 1200-meter
Simulation time	400s
Pause time (s)	0, 100, 200, 300, 400

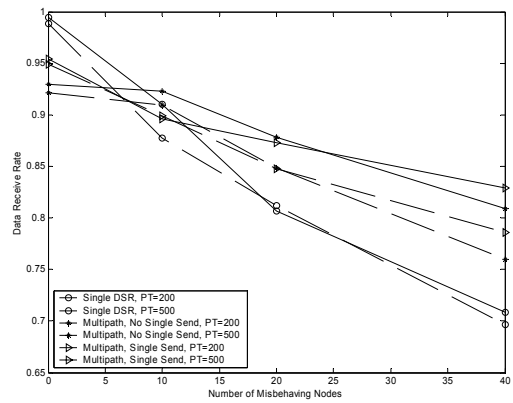

Fig. 5. Decrease in Data Receive Rate for Dropping Data.

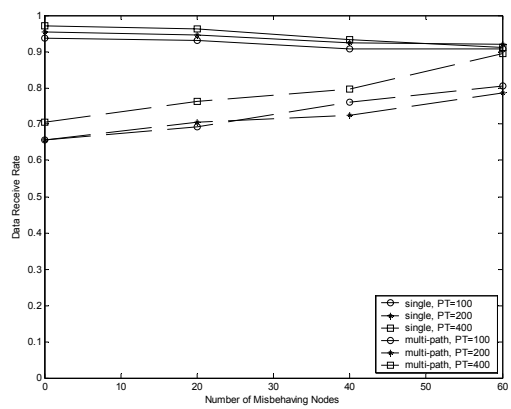

Fig. 6. Data Receive Rate for Colluded Dropping.

Fig. 6 shows the comparisons of the data receive rates of proposed scheme and the single path DSR under the colluded dropping circumstance. When the misbehaving nodes drop the transmitted data colluding, with the increase of the misbehaving node, the data receive rate of the single path DSR decreases, but that of the proposed multipath routing scheme increases. As the misbehaving nodes in an area would connect with each other, with more misbehavior nodes in the network, it becomes harder to find two node-disjoint paths without misbehaving nodes on the data transmission path. Thus, the number of sent data packets decreases. As the proposed scheme can detect the colluded dropping and notify the source switch to other path in time, more data packets sent would attend the destination. The data receive rate increases accordingly. The result that data receive rate when pause time is 400 seconds is larger than that when pause time is 100 second shows that the proposed scheme is more suitable for a relatively static ad hoc network. The simulation results also

show that the data transmission paths are forced to be with length *1* or *2* hops to avoid colluded dropping. Thus, only when the destination is within *2* hops of the source can two node-disjoint paths be selected.

V. Concluding Remarks

In this paper, based on the performance analysis of multipath data transmission in ad hoc networks, we have presented a novel secure data transmission scheme that utilizes multiple routing algorithms to secure data transmission in ad hoc networks. The performance of the proposed scheme and a simple derivation under normal and adverse environments has been studied by means of simulation and discussed in details. Following are the features of the proposed scheme.

- *Security improvement using multipath routing*. This scheme needs two node-disjoint paths and uses one of them to transmit data. It can defend against misbehavior conducted by one individual or some cooperating misbehaving nodes in ad hoc networks. Its performance is evaluated under both normal and adverse environments. The data receive rate is improved around 20% over the single path DSR when a single misbehaving node conducts dropping data. The data receive rate increases with the number of misbehaving nodes when misbehaving nodes conduct colluded dropping in the network.
- *Expendable scheme.* The derivation discussed above is only the simplest modification of the proposed scheme. It can be modified in various ways to provide further protection to the network. For example, a reputation system can be introduced into this scheme.
- *Moderate overhead.* It provides security protection to data transmission in ad hoc networks at expense of moderate overhead introduced by using multipath routing and new control packets in the scheme.

It should be mentioned that sybil attack [5], in which a single node presents multiple identities to other nodes in the network, can reduce the effectiveness of multipath routing and may make this scheme fail to work. However, our scheme in combination with other countermeasures, such as radio resource testing, position verification and random key predistribution, will be able to defend from sybil attack [9]. On the other hand, in a network implementing topology control protocol, as two node-disjoint routes can be achieved more efficiently, this scheme would show to be more beneficial.

If there are a very small number of misbehaving nodes in the ad hoc network, the single path routing scheme may be able to provide an adequate performance. When a number of misbehaving nodes are present, especially when they can cooperate with each other, and secure data transmission is a great concern, our scheme can be used to improve and/or maintain the performance of the ad hoc network.

Acknowledgement

The authors thank the reviewers for their helpful comments. And this work was sponsored in part by the Boeing Centennial Endowed Chair, School of Electrical Engineering and Computer Science, Washington State University.

Reference

[1] K. Balakrishnan, J. Deng, P. K. Varshney, "TWOACK: preventing selfish in mobile ad hoc networks," *Proc. WCNC'05*, Vol. 4, 13-17 New Orleans, LA, USA, March, 13-17, 2005, pp. 2137 – 2142.

[2] 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.

[3] C. M. Cordeiro, S. R. Das, and D. P. Agrawal, "COPAS: dynamic contention-balancing to enhance the performance of TCP over multi-hop wireless networks," *Proceedings of the International Conference on Computer Communication and Networks,* Miami, Florida, Oct. 2002, pp. 382-387.

[4] Y. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless ad hoc networks", *Proc. INFOCOM' 03*, IEEE, San Francisco, CA, April 2003, pp. 1976- 1986.

[5] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, May, 2003, pp. 113-127.

[6] S. Lee, M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks", *Proc. IEEE ICC 2001*, pp. 3201-3205, 2001.

[7] W. Lou, W. Liu and Y. Fang, "SPREAD: enhancing data confidentiality in mobile ad hoc networks", *Proc. IEEE INFOCOM 2004,* Volume 4, 7-11 pp. 2404 – 2413, Hong Kong, China, March 2004.

[8] S. Marti, T.J.Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", *Proc. MobiCom 2000,* ACM, Boston, MA, August 2000, pp. 255-265.

[9] J. Newsome, E. Shi, D. Song, A. Perrig, "The sybil attack in sensor networks: analysis and defenses," *Proc. IPSN' 04*, April, 2004, Berkely, California, pp. 259-268.

[10] P. Papadimitratos and Z. J. Haas, "Secure data transmission in mobile ad hoc networks", *Proc. WiSe'03,* San Diego, CA, Sep. 2003, pp. 41-50.

[11] V. D. Park and M. S. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks", *Proc. IEEE INFOCOM'97,* 04, 1997. Vol. 3, 7-11 April 1997, pp.1405 – 1413.

[12] M. R. Pearlman, Z. J. Haas, P. Scholander, S. S. Tabrizi, "On the impact of alternate path routing for load balancing in mobile ad hoc networks", *Proc. ACM MobiHoc 2001*, pp. 3-10, 2001.

[13] K. Wu, J. Harms, "Performance study of a multi-path routing method for wireless mobile ad hoc networks", *Proc. MASCOTS' 01*, 2001, pp. 99-107.

[14] X. Zeng, R. Bagrodia, M. Gerla, "GloMoSim: a library for parallel simulation of large-scale wireless networks", *Proc. 12th Workshop on Parallel and Distributed Simulation*, May 26-29, 1998, in Banff, Alberta, Canada.

[15] L. Zhou, Z. J. Haas, "Securing ad hoc networks", *IEEE Network*, Nov/Dec 1999, pp 24-30.