A Simulation Study of Security Performance Using Multipath Routing in Ad Hoc Networks

Wenjing Lou Wei Liu Yuguang Fang
Department of Electrical and Computer Engineering
University of Florida
Gainesville, FL 32611
Email: {wjlou@, liuw@, fang@ece.}ufl.edu

Abstract – **In this paper, we investigate the security performance of the SPREAD scheme, which we proposed as a complementary mechanism to enhance data confidentiality in a mobile ad hoc network (MANET). SPREAD is based on two principles, secret sharing and multipath routing. By a secret sharing scheme, a secret message can be divided into multiple shares; then by multipath routing, the shares can be delivered to the destination via multiple paths. Improved security is expected because an adversary (adversaries) will have more difficulty in collecting enough shares to compromise the secret message. As the broadcast wireless channel of a MANET has a significant impact on the performance of multipath routing, we examine the performance of SPREAD based on the shared single wireless channel model by simulation. Our results show that SPREAD scheme is effective in reducing the message compromising and eavesdropping probability. The impacts of node mobility and different share allocations on the performance of SPREAD are also investigated.**

Index terms — multipath routing, ad hoc network, security, simulation

I. INTRODUCTION

Security is a critical issue in a mobile ad hoc network because the primary applications of ad hoc networks are the military applications, such as the tactical communications in a battlefield, where the environment is hostile and the operation is security-sensitive. As compared with a fixed or a wired network, the characteristics of an ad hoc network pose many new challenges in security. For example, the wireless channels are more susceptible to various forms of attacks such as passive eavesdropping, active signal interference, and jamming. The co-operative nature of ad hoc protocols makes it more vulnerable to data tampering, impersonation, and denial of services. The lack of a fixed infrastructure restricts the applicability of some conventional security solutions, such as a Public Key Infrastructure (PKI), which relies on a centralized trusted authority, and the intrusion detection system, which needs a concentration point to collect audit data. The limited resources of mobile devices, such as the battery power, also limit the practical deployment of more comprehensive security schemes in an ad hoc network. Finally, the continuous and unpredictable ad hoc mobility clouds the distinction between normalcy and anomaly, thus makes the detection of the malicious behavior difficult.

A few research works have been done to address the security issues in ad hoc networks. Security issues that have been addressed particularly for ad hoc networks include key management [1], secure routing protocols [2], handling node misbehavior [3], preventing traffic analysis, and so on [4]. In this paper, we address the data confidentiality service in an ad hoc network. The data confidentiality is the protection of data from passive attacks such as eavesdropping while they are transmitted across the network. The wireless channel in a hostile environment is vulnerable to various forms of attacks, particularly the eavesdropping. A more severe problem in a MANET is that mobile nodes might be compromised themselves (e.g., nodes be captured in a battle field scenario) and subsequently be used to intercept secret information relayed by them. In [5], we proposed a SPREAD (Secure Protocol for REliable dAta Delivery) scheme to statistically enhance the data confidentiality service in an ad hoc network. SPREAD is based on secret sharing and multipath routing. Multipath routing has been extensively studied in a wired network context for aggregating bandwidth, reducing blocking probability, and increasing the fault tolerance, etc. [12]. However, the shared wireless channel has a significant impact on the performance of multipath routing [9]. In this paper, we study the security performance of SPREAD under single shared wireless channel by simulation.

This paper is organized as follows. In section II, we give a brief overview of the proposed SPREAD scheme. In section III, we describe two wireless channel models for MANETs and discuss their impacts on the security performance of SPREAD. The simulation results are reported in section IV. Conclusion is drawn and future work is proposed in section V.

II. OVERVIEW OF THE SPREAD SCHEME

The SPREAD scheme combines the secret sharing and multipath routing to reduce the message interception caused by compromised nodes or eavesdropping. In our SPREAD scheme, a secret message is first divided into multiple *(N)* pieces (called shares or shadows) using a *(T,N)* threshold secret sharing scheme such that from any *T* or more shares, it can easily recover the message, while from any *T-1* or fewer shares, it should be impossible to recover the message.

This work was supported in part by the Office of Naval Research Young Investigator Award under grant N000140210464 and the Office of Naval Research under grant N000140210554.

Shamir's Lagrange interpolating polynomial scheme [6] is used in our SPREAD scheme to generate the message shares. Details about dividing and reconstructing the message by secret sharing scheme can be found in [7]. Then using multipath routing, SPREAD delivers the shares across the network via multiple disjoint paths. The technique used to find the multiple most secure paths is discussed in [5]. Finally the destination node reconstructs the original message upon receiving T or more shares. It will recover the original message from any T correct shares but will fail if the number of correct shares is less than T.

We apply link encryption in the scenario where SPREAD is applied. Each link uses a different encryption key which is negotiated between the two neighboring nodes (e.g. using the Diffie-Hellman key exchange protocol). To compromise the message, the adversary may either compromise the nodes thus intercept all the secrets transmitted over those nodes, or eavesdrop the transmission of other nodes and then try brute-force type of decryption. From network point of view, if a whole message follows a single path to its destination, an adversary can intercept all the necessary information to recover that message by compromising any one of the nodes along the path. However, with the SPREAD scheme, except the source and destination nodes, the adversary must compromise a number of intermediate nodes on a number of independent paths to obtain the minimum required (T) shares. Consider a scenario of (*3, 3*) secret sharing and the multipath routing as illustrated in Figure 1. It is clear that except the source and destination, no single node could possess all the necessary information to recover the message. In other word, an adversary must compromise at least 3 nodes on three different paths to be able to compromise the message. Significantly reduced message interception ratio can be expected.

Share allocation is another major design issue in SPREAD. Share allocation discusses how to select the paths, how to choose an appropriate value of (T,N), and how to allocate the shares onto each selected path such that the maximum security can be achieved. The simplest and most intuitive share allocation scheme is to choose N as the number of available paths, apply (N,N) secret sharing, and allocate one share onto each path. This will achieve the desired maximum security with least processing cost. However, in an ad hoc network, wireless links are instable and the topology changes frequently. Sometimes packets might be dropped. In the case that packet loss does occur, this type of non-redundant share allocation will disable the reconstruction of the message at the intended destination. To deal with this problem, we introduce redundant (i.e. $T<N$) SPREAD scheme to improve the reliability. In [8] we discussed the optimal share allocations. We formulated the share allocation into a constrained optimization problem, with the objective to minimize the message compromising probability. Our investigation to the optimal share allocation reveals that, by choosing an appropriate (T,N) value and allocating the shares onto each path carefully, we could improve the reliability by tolerating certain packet loss without sacrificing the security. The

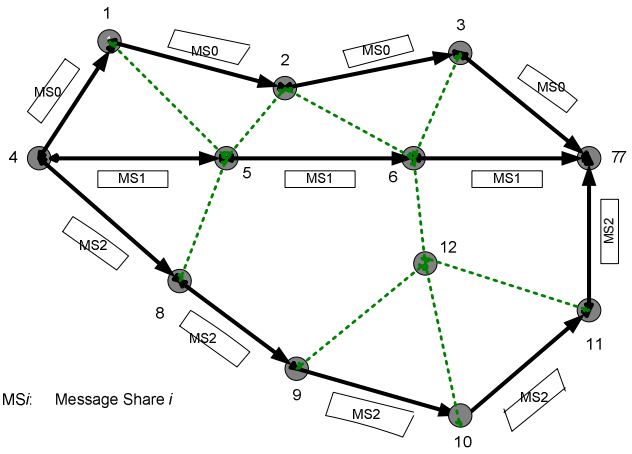

Figure 1. Illustration of multipath routing

maximum redundancy we can add to the SPREAD scheme without sacrificing security is identified as $r < 1/m \ (m \geq 2)$, where $r = 1 - T/N$ is the redundancy factor and m is the number of paths selected to deliver the message. The optimal share allocation is proposed. Basically any allocation that conforms to the constraints

$$\begin{cases} N - T + 1 \leq n_i \leq T - 1, & \text{i} = 1,..., \text{m} \\ \sum_{i=1}^{M} n_i = N \end{cases}$$

is an optimal share allocation in terms of security. More details about share allocation can be found in [8].

III. MULTIPATH ROUTING

Nodes in an ad hoc network use wireless channels to communicate with each other. There are two types of physical layer channel allocation schemes, single-channel and multiple-channel [9]. Based on the channel allocation schemes, the radio links in an ad hoc network may have very different characteristics. These differences have significant impacts on the performance of multipath routing in a MANET.

A. Multiple-Channel Model

In the multiple-channel model, we assume that we may have multiple independent logical channels among nodes so that even multiple nodes in their transmission ranges (they are neighbors), multiple links can be deployed for establishing independent multiple paths among them in the high layers. Such scenario may be possible in various situations: when each node is equipped with multiple transmitters and receivers that can work independently and simultaneously, or when each node is equipped by directional antenna, or when each link is assigned a locally unique channel that is distinct from those channels used by its two-hop neighbors to avoid collision. With this model, each link's communication activity is independent of those of its neighbors. The concurrent data transmission in overlapped neighborhoods is supported. The network layer topology is sufficient to carry out the analysis of routing protocols. The node-disjointness is sufficient to

imply the independence of paths. Since each link uses independent channel, only the intended receiver can receive the message shares. Other neighbors of the transmitter would not be able to overhear the information. Consider a scenario of (*3, 3*) secret sharing and the multipath routing as illustrated in figure 1. It is clear that except the source and destination, no single node could possess all the necessary information to recover the message. In other word, adversaries must collude to compromise a message, e.g., they must compromise or eavesdrop at least three nodes on three different paths to be able to recover the message (Here we do not consider the source and destination nodes because our SPREAD protocol aims to improve the data confidentiality while they are transmitted across the network. The protection of each particular node is a separated issue and is not in the scope of this paper). If we assume that the compromising of each node is independent, it is intuitive to derive that the probability that a message is compromised/eavesdropped decreases exponentially with the number of paths used to spread the traffic.

B. Single-Channel Model

In the single-channel allocation model, all the nodes are assumed to use a single shared channel to communicate with each other. All nodes transmit to the same shared channel. If more than one neighboring nodes transmit at the same time, a collision will occur at the receiving end. Nodes also listen to the same shared channel. When one node transmits, all its neighboring nodes can hear that transmission. In this model, a media access control (MAC) protocol, such as IEEE 802.11, is required to coordinate the transmission of nodes, thus the collision can be avoided. This shared channel model is commonly adopted in the current ad hoc networks literature. Again assume (*3,3*) secret sharing and consider the multipath routing as illustrated in figure 1, however here we assume a single-channel implementation. Except the source and destination, there are totally 3 intermediate nodes (1,5,8) who could overhear all the necessary shares in the multipath scenario, compared with totally 7 such nodes (1,2,3,5,6,8,12) with the single shortest path routing (route 4-5-6-7). The guaranteed security improvement by SPREAD is not so obvious in single channel implementation due to the correlation among routes. It can be intuitively proved as follows. Assume an *M*-path routing is used and there exist totally L_M nodes which are able to collect all *M* shares. Then, if we keep the first *M* paths and add the (*M*+1)*th* path, the set of nodes which are able to collect all (*M*+1) shares has to be a subset of nodes which are able to collect the first *M* shares. Thus $L_{M+1} \le L_M$ is guaranteed.

Obviously, the security in the single-channel ad hoc network is a more challenging task. We notice that, except the source and destination, the neighbors of the source node can always hear all the shares. Thus, an eavesdropper in the neighborhood of source node or destination node may have the same privilege getting all shares. However, in MANET environments, nodes are highly mobile, unless the eavesdropper keeps tracking the source node or the destination node accurately, the security enhancement is still valid. In addition, our scheme is on top of underlying encryption schemes, the eavesdropper may still have hard time to decrypt the message. Our security enhancement is in the statistical sense. We will show the performance of multipath routing based on the single-channel model by simulation in the following section.

IV. Simulation and Results

A. Simulation Framework

The simulation of our SPREAD protocol is implemented using OPNET [10]. A mobile ad hoc network consisting of 100 nodes in a simulation area of 1000m×1000m is simulated. The link layer model is the Distributed Coordination Function (DCF) of the IEEE 802.11 wireless LAN standard. The radio model uses the frequency hopping spread spectrum technology with 2 Mbps capacity. The radio propagation range for each node is 250 meters.

The random waypoint mobility model is used in the simulation. Nodes are initially placed in the simulation territory randomly. After stops for a predefined pause time, each node selects a destination randomly within the simulated territory, then moves to that destination at a speed uniformly distributed in [vmin, vmax] m/sec. The stop and move behavior is repeated for the duration of the simulation. In our simulations, [vmin, vmax] is fixed to [0,20]. The different node mobility levels are achieved by changing the values of pause time.

As we discussed in [5], our multiple paths selection could be based on the partial network topology discovered by any underlying multipath routing protocols. To factor out the effect of routing protocols, in the simulation we adopt a DSR-like "God" routing protocol. The "God" routing protocol keeps the fundamental features of the on-demand routing protocols. Whenever a node has a message to be transmitted and there is no known path to that destination, the "God" process refreshes its network topology data structure to reflect the most up-to-date changes (mimic the route discovery procedure of DSR). The multipath finding algorithm is then executed to find the desired number of node disjoint paths (*M,* we set M=1,2,3,4,5 respectively in each simulation run; we also set the maximum length of acceptable path to 8). Then the message will be divided into 10 shares and sent to the destination via the *M* paths. We use the following simple share allocations. For *M*=1, $\underline{n}$=[10]; *M*=2, $\underline{n}$=[5 5]; *M*=3, $\underline{n}$=[4 3 3]; *M*=4, $\underline{n}$=[3 3 2 2]; *M*=5, $\underline{n}$=[2 2 2 2 2], where $\underline{n}=[n_1\ n_2\ \ldots\ n_M]$ indicates that the number of shares allocated to path *i* is n_i. The routing in the intermediate nodes is achieved by source routing technique. A route cache is kept in each node to save the paths used. Once the paths to a certain destination are calculated, they are used till a link error occurs. When a link error occurs, an interrupt will be delivered to source node and the paths will be recalculated for the next message (mimic the route maintenance mechanism in DSR).

Two sets of simulations are executed. In the first set, each node is assumed equally likely to be compromised with

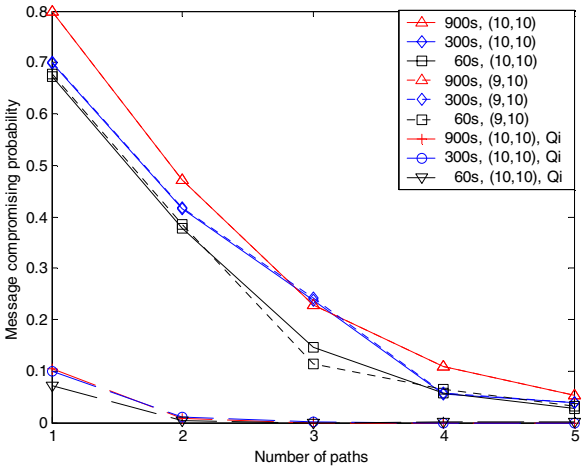

Figure 2 Message compromising probability

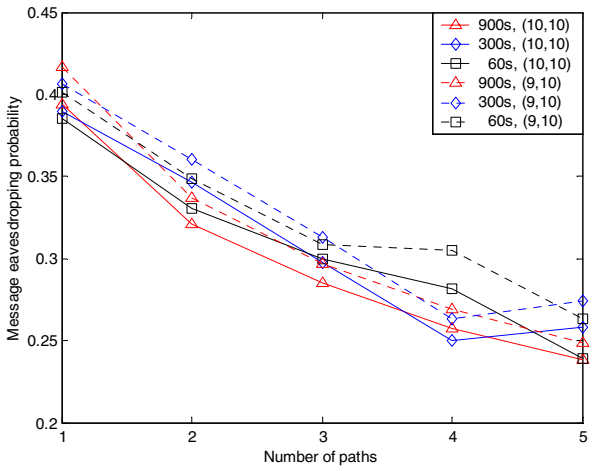

Figure 3 Message eavesdropping probability

probability q_i=0.152. In the second set of simulation, each node is assigned a probability randomly: 10% of nodes with probability q_i =0.50, 30% of nodes with q_i =0.20, 40% of nodes with q_i =0.10, and 20% of nodes with q_i =0.01. In the first set, all the links are of same cost. In the second set, we use the following link cost function proposed in [5] to define the link cost between node i and j as $c_{ij} = -\log\sqrt{(1-q_i)(1-q_j)}$. This link cost definition can convert the node security property into an additive link cost function thus the shortest path algorithm can be used to find the most secure path.

In our simulation, there are totally 15 randomly selected compromised nodes. Other 85 nodes are good nodes. Messages are generated at each good node independently following a Poisson arrival process. The destination for each packet is chosen randomly among the good nodes. We require that the destination is at least 3 hops away from source. Each simulation is executed for 15 simulated minutes.

B. Security Performance Metrics

In our simulation, each message share is transmitted over the network in the form of a network layer packet using source routing technique. Besides the source routing information, it also carries with it the following information, a globally unique *message_ID*, the (*T*,*N*) values used to generate this share, and a *share_ID* which identifies this particular share among the total *N* shares for that message.

First we define the message compromising probability. Since we assume link encryption, if one share is relayed by a compromised node, we consider that the share is compromised. If *T* out of *N* shares are compromised, we consider the message is compromised. Obviously, the individual attack on message compromising is zero when multiple (*M*>1) paths are used because no single node will relay necessary shares according to the distributed nature of the delivery scheme. In our simulation, we also consider the collusion attack. That is, we assume full collaboration among compromised nodes and they can combine the compromised shares together to recover a message. If at least *T* shares of a message are compromised by them, the message is considered compromised. Figure 2 shows this colluded message compromising probability. Notation {900s, (9,10), Qi} means the curve is obtained when pause time in the mobility model is set to 900s, (*T*,*N*) is set to (9,10), and nodes are assumed with different probabilities (q_i) to be compromised; Without Qi it means that nodes are assumed equally likely to be compromised. We observe that the probability drops quickly (actually exponentially fast) with the increase of the number of paths used. This result verifies the effectiveness of our SPREAD idea. We also noticed that when nodes are with different security level (q_i), the security related cost function helps to select more secure paths that further decrease this probability significantly.

We also examine the message eavesdropping probability. As we use a single shared channel, when one node transmits a packet, all its neighbors would be able to overhear that packet. In our simulation, each compromised node also overhears packets and records *message_ID* and *share_ID* of the received packet. If the node has overheard *T* or more different shares for a particular message, this message is considered eavesdropped. Figure 3 plots the message eavesdropping probability for individual node attack. That is, each node works on its own to collect the *T* shares. It is observed that, with the increase of the number of paths, this probability decreases. However, the decrease becomes less significant when more paths are used. In fact, there is a lower bound of this probability because anyone sits within the transmission range of the source node would be able to overhear all the shares. Of course, this probability is the one that an adversary might overhear a message, it does not mean that the message can be compromised because the message shares are encrypted as well. Again, this verifies that the SPREAD idea makes it harder for an enemy to collect enough data to break the secret. The message eavesdropping probability for collusion attack is pretty high (close to 1) because in our simulation, we have about 15 compromised nodes among the totally 100 nodes. The simulation results with Qi is very

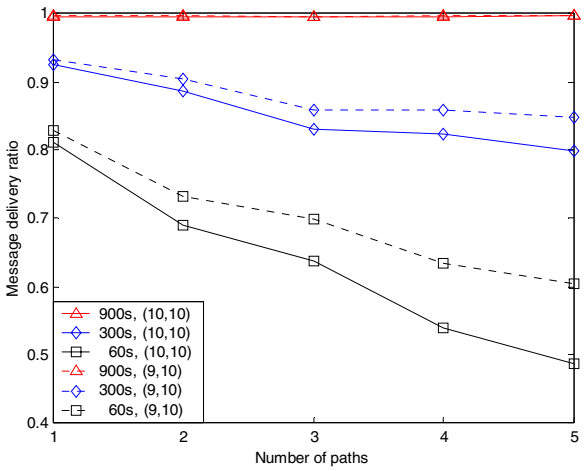

Figure 4. Message delivery ratio

similar to the ones without Qi as shown in figure 3, thus not included due to the space limitation. It implies that the secure paths selected based on physical security of each node have little impact on the eavesdropping of broadcast channels.

In both figure 2 and 3, we show the probabilities with different node mobility. Another interesting observation is that SPREAD scheme achieves slightly better security when node's mobility is higher. This can be explained as when shares take different paths, there is a time delay between the arrivals of different shares onto one particular node. If nodes move faster, they might move out of the region before all the shares are captured by a compromised node. The node mobility actually helps security in this sense. Therefore the overall security performance improves slightly with the node mobility.

C. *Impact of Share Allocation Schemes*

As we mentioned before, we designed optimal share allocation scheme which is able to provide certain degree of reliability without scarifying the security. In this paper, we compare a non-redundant (10,10) secret sharing and a redundant (9,10) secret sharing. As expected, we observe in figure 2, the two secret sharing schemes, (9,10) and (10,10), achieve the same level of message compromising probability. While for message eavesdropping probability shown in figure 3, the non-redundant scheme achieves better performance.

The redundant SPREAD scheme is design mainly for the reliability of the message delivery. Figure 4 compares the message delivery ratio of non-redundant (10,10) and redundant (9,10) SPREAD. A message is considered as received when at least T shares are successfully received at the intended destination. It can be observed that the redundant SPREAD improves the message delivery ratio significantly.

Multipath routing has been suggested to be a promising technique to improve the reliability in mobile ad hoc networks because the use of multiple paths could diminish the effect of unreliable wireless links and the constant topological changes [11]. The improving also depends on the proper allocation of packets onto each path and proper adding of redundancy. In our simulation, we focus on the security performance rather than the reliability performance. We observed that when multipath routing is used, the message delivery ratio is actually degraded. This is mainly because the closely correlated paths cause severe collisions at MAC layer. Those collisions mostly come from the shares of the same message. As implied by the simulation results, the correlation between routes has a significant impact on the network performance of SPREAD scheme. Our future work will be focused on the design of a distributed routing protocol that aims to find multiple least correlated paths efficiently.

V. Conclusions and Future Work

Security is a critical issue in an ad hoc network. In this paper we investigate by simulation the performance of the SPREAD scheme that we proposed as a complementary mechanism to enhance the data confidentiality service in an ad hoc network. The SPREAD scheme is based on the idea to distribute a secret among multiple independent paths while it is transmitted across the network. Through simulation, the effectiveness of SPREAD in improving network security is verified. We show that the message compromising and eavesdropping probabilities can be reduced effectively. However, in a shared-channel ad hoc network, correlation among routes widely exists. Our simulation also shows that multipath routing causes more collision among correlated routes themselves thus degrades network performance such as packet delivery ratio. In our future work, we will be focusing on developing multipath routing protocols which take into consideration of the network performance as well.

References

[1]. L. Zhou, Z.J. Haas, "Securing ad hoc networks", *IEEE Network Magazine*, Nov 1999

[2]. Y.-C. Hu, A. Perrig and D. B. Johnson, "Ariadne : a secure on-demand routing protocol for ad hoc networks," *MobiCom* 2002, Sep 2002

[3]. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", *MobiCom* 2000, Boston, MA, Aug 2000

[4]. W. Lou, Y. Fang, "A survey of wireless security in mobile ad hoc networks: challenges and available solutions", book chapter in *Ad Hoc Wireless Networking*, Kluwer, May 2003

[5]. W. Lou, Y. Fang, "Securing data delivery in ad hoc networks", *International Workshop on Cryptology and Network Security (CANS'03),* Miami, FL, Sep 2003

[6]. A. Shamir, "How to share a secret", *Communications of the ACM*, 22(11):612-613, Nov 1979

[7]. W. Lou, Y. Fang, "A multipath routing approach for secure data delivery", *IEEE Milcom'01*, Oct 2001

[8]. W. Lou, W. Liu, Y. Fang, "SPREAD: Improving network security by multipath routing", *IEEE Milcom'03*, Boston, MA, Oct 2003

[9]. M.R. Pearlman, Z.J. Haas, P. Sholander, S. S. Tabrizi, "On the impact of alternate path routing for load balancing in mobile ad hoc networks", *MobiHOC*, 2000

[10]. http://www.opnet.com

[11]. A. Tsirigos, Z.J. Haas, "Multipath routing in the presence of frequent topological changes", *IEEE Communication Magazine*, Nov 2001

[12]. E. Gustafsson, G. Karlsson, "A literature survey on traffic dispersion", *IEEE Networks*, Mar/Apr 1997, pp.28-36