A Reliable Multi-Path Routing Protocol for Ad-Hoc Network

Li-Ping Chou* and Chin-Chi Hsu
Department of Computer Science
and Information Engineering
National Taiwan University
Taipei, Taiwan

Fan Wu
Department of Information Management
National Chung Cheng University
Chia-Yi, Taiwan

Abstract

Ad-hoc networks are a new wireless networking paradigm for mobile hosts. Unlike conventional wireless networks, ad-hoc networks have no fixed network infrastructure or administrative support. The topology of the network changes dynamically as mobile nodes join or depart the network or radio links between nodes become unusable. In this paper we propose some efficient multi-path approaches that provide more secure routing schemes for ad-hoc network than previous ones. Within these approaches, more than one routing paths are selected. With the underlying coding technique, it can guarantee security against some malicious parties(it depends on how robust system is.) Moreover, we apply these schemes into existing ad-hoc network routing protocols, table-driven and on-demand routing algorithms. Finally, we derive the relation between some probabilities on our algorithms.

Keywords: Ad-hoc Networking, Dynamic Routing, Mobile Networking, Wire-less Networks, Distributed algorithm.

1 Introduction

An ad-hoc network is temporarily formed by a group of mobile hosts communicating over wireless media without any fixed network interaction and centralized administration. In the infrastructure, all the mobile device communicate with other mobile devices in a wireless multi-hop routing style. All the mobile devices behave as routers in the ad-hoc network. Because the routers are mobile, the network topology is changed frequently by some events among mobile devices. For instance, the mobile devices may move around or switch on and off. The routing scheme in ad-hoc networks is more challenging than traditional networks in terms of dynamic network topology.

We can image that the ad-hoc communication is a special computing environment with highly possible link failure and site failure. In any time, we could not know the actual topology of the network, even many scholars proposed many approach to maintain routing tables or something like that.

Rabin[16] proposed the very practical algorithm "Information Dispersal Algorithm (IDA)", which can not only achieve the reliability but also security characteristics by using a much overhead of redundancy and by keeping only partial information at every site. The main idea is to split the information into n distinct pieces by using a secrete key. Then Sender can transmit those n pieces by any media carrier. Receiver can reconstruct the original information from any m of n pieces, where $m \leq n$.

The IDA algorithm can provide high availability and fault-tolerance, since it tolerates up to $(n - m)$ failures.

It also provides another property of confidentiality of the dispersed information. As a mater of fact, it is hard to get any clue about the original information unless at least m pieces from the dispersed file are collected. Even if this happens, it is provably very difficult, since it is provably very difficult to reconstruct the original file unless the secret keys are known.

This paper is organized as follows; Section 2 describes some previous works about multi-path routing. Section 3 demonstrates the key idea of IDA. The key point of new multi-path routing scheme is proposed in section 4. Section 5 shows an important relationship between some parameters.

2 Previous Works on Ad-Hoc Multi-path Routing

The application of multi-path techniques in mobile ad-hoc networks seems natural, as multi-path routing allows to diminish the effect of unreliable wireless links and the constantly changing topology. Although these

*Corresponding author, Tel:886-2-29851551, Fax:886-2-89835212, clp@csie.ntu.edu.tw

protocols build multiple routes on demand (most of them use DSR [11]), the traffic is not distributed into multi-paths; only one route is primarily used and alternate paths are utilized only when the primary route is broken.

Lee and Gerla [12] propose Split Multi-path Routing (SMR). It is an on-demand routing protocol that builds multiple routes using request/reply cycles. The main goal of SMR is to build maximally disjoint multiple paths. They want to construct maximally disjoint routes to prevent certain nodes from being congested, and to utilize the available network resources efficiently. Their approach has a disadvantage of transmitting more RREQ (Route Request) packets, but it enables us to discover maximally disjoint routes.

Nasipuri, Castañeda and Das [14] also develop a multi-path extension to DSR. They first consider the situation where the destination replies to a selected set of queries. Note that many copies of the flooded query message arrive at the destination via different routes. The queries that are replied to are those that carry a source route that is link-wise disjoint from the primary source route.

Wu and Harms [20] declare there are three criteria: node-disjoint, small length difference, small correlation factor between any two of the multiple paths. They define a metric, *correlation factor* to describe the interference of traffic between two node-disjoint paths. The correlation factor of two node-disjoint paths is defined as the number of the links connecting the two paths. Their on-demand multi-path calculation method based on the heuristic redirection of RREP packets.

Tsirigos and Haas [19] propose a more complicated routing protocol combining with diversity coding. They also split the information among the multitude of paths, such that it can guarantee the high successful probability that the crucial part of the information is received at the destination.

3 Concepts of Information Dispersal Algorithm

Many researchers focused on the MAC-layer of ad-hoc routing. Most of them use the previous routing schemes for TCP/IP and so on [18]. Until the Rabin [16] proposed amazing information dispersal algorithm (IDA). Not only it can be applied to distributed computing environment, but also other computer engineering application.

Rabin's work was subsequently simplified and strengthened by Håstad, Leighton and Newman [8] and Lyuu [13]. An earlier and similar approach to informa-

tion dispersal is described by Preparata [15]. A good references on fault tolerance in hypercube network can be found in the paper of Aiello and Leighton [1].

Bestavros is the first scholar that apply IDA scheme to implement VLSI and RAID-like application [4][3]. He also applied it to the communication with QoS issue [5].

In this section, we show how the IDA works. Let I be the original information we want to transmit. The original information can be encoded as a 4-bits data sequence. In order to disperse this sequence, we choose a key, which contains contains n vectors, each of length m . In fact these keys must subject to linear independence property. Let D_{nm} be the matrix contains the key. D_{nm} is a mapping from an m -dimensional space to an n -dimensional space.

To split the original information I , we use the transformation D_{nm} to map each sequence of m elements from I into a new sequence of n elements, such that, for each m elements of I we send one element to each of the n paths. Therefore, to split the information I we will need to send $\frac{|I|}{m}$ elements to each of the n paths.

For any integer $s > 1$, the finite field $GF(2^s)$ consists of all s -bit binary strings. Each s -bit binary string $a = a_0a_1 \cdots a_{s-1}$ corresponds naturally to an $(s-1)$ -degree polynomial $a(x) = a_0 + a_1x + \cdots + a_{s-1}x^{s-1}$. Addition and multiplication operations of elements over the field are computed by the same operation on the corresponding polynomials, where modulo an 2^s irreducible polynomial (one that cannot be divided by any polynomial of $2^s - 1$ or lesser degree.) Every coefficients are also evaluated modulo 2.

For example, if $s = 4$, then $GF(2^4)$ consists of the following 16 elements:

0000	0
0001	1
0010	x
0011	$x + 1$
0100	x^2
0101	$x^2 + 1$
0110	$x^2 + x$
0111	$x^2 + x + 1$
1000	x^3
1001	$x^3 + 1$
1010	$x^3 + x$
1011	$x^3 + x + 1$
1100	$x^3 + x^2$
1101	$x^3 + x^2 + 1$
1110	$x^3 + x^2 + x$
1111	$x^3 + x^2 + x + 1$

Following examples show the coefficients are evaluated by modulo 2 and it also evaluated modulo by $x^4 + x + 1$,

the irreducible 4th polynomial.

$$\begin{aligned} 4 + 7 &= (x^2) + (x^2 + x + 1) \\ &\equiv (x + 1) \pmod{x^4 + x + 1} \\ &= 3 \end{aligned}$$

Let's see another example, if $s = 2$ we choose $x^2 + x + 1$ to be the irreducible polynomial of degree 2, then

$$\begin{aligned} x \cdot (x + 1) &= (x^2) + x \\ &\equiv (x^2 + x) \pmod{x^2 + x + 1} \\ &= 1 \end{aligned}$$

Hence, $x^{-1} = x + 1$ in this field.

3.1 The Disperse part of IDA

We define

$$D_{nm} = \begin{bmatrix} 1 & \phi_1 & \phi_1^2 & \cdots & \phi_1^{m-1} \\ 1 & \phi_2 & \phi_2^2 & \cdots & \phi_2^{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \phi_n & \phi_n^2 & \cdots & \phi_n^{m-1} \end{bmatrix}$$

to be the $n \times m$ matrix whose i, j entry is ϕ_i^{j-1} , where the ϕ_i are distinct elements of $GF(2^s)$.

Then we partition the original information B bits of P into m subpackets $P'_1, P'_2, \dots, P'_m$, each with $\frac{B}{m}$ bits. In polynomial forms is

$$P'_i = \sum_{j=1}^m \phi_i^{j-1} P_j$$

for $1 \leq i \leq m$, That is,

$$\begin{bmatrix} P'_1 \\ P'_2 \\ \vdots \\ P'_m \end{bmatrix} = D_{nm} \begin{bmatrix} P_1 \\ P_2 \\ \vdots \\ P_m \end{bmatrix}$$

3.2 The Reconstruct part of IDA

Given any collection of m of the subpackets P'_i , we can reconstruct original packet P as follows,

For any $i_1, i_2, \dots, i_m$, we know that

$$\begin{bmatrix} P_{i_1} \\ P_{i_2} \\ \vdots \\ P_{i_m} \end{bmatrix} = \begin{bmatrix} 1 & \phi_{i_1} & \phi_{i_1}^2 & \cdots & \phi_{i_1}^{m-1} \\ 1 & \phi_{i_2} & \phi_{i_2}^2 & \cdots & \phi_{i_2}^{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \phi_{i_m} & \phi_{i_m}^2 & \cdots & \phi_{i_m}^{m-1} \end{bmatrix} \begin{bmatrix} P'_{i_1} \\ P'_{i_2} \\ \vdots \\ P'_{i_m} \end{bmatrix}$$

Because any subset of m rows of D_{nm} is invertible[16][4], so we can retrieve $P'_{i_1}, P'_{i_2}, \dots, P'_{i_m}$ by solving the system of equations over $GF(2^s)$, therefore obtaining the bits of the original packet P .

4 Highly Reliable Routing Framework(HRRF) for Ad-Hoc network

Although the original IDA paper provide a scheme to construct the highly reliable routing with multiple paths. It does not consider the scenario of ad-hoc network, for example the path selection extension and routing table maintenance. In the following section, we would deal with those problems.

4.1 IDA-based Algorithm over Ad-Hoc Communication

We extend some traditional ad-hoc routing protocols to highly-reliable routing scheme by adding some mechanism to which kind of the original protocol it belongs.

All mobile devices should establish the α, β, m parameters according to the network topology variance, α is the possibility that the devices handoff, β the possibility that some paths are not totally disjoint and m is the how many parts of information the network wants to disperse. For example, we can image the m should be related with the logarithm function of α and β individually.

$$m = \lfloor \alpha^{-1}(\log(\alpha^{-1})) + \beta^{-1} \log(\beta^{-1}) \rfloor$$

Remark: This equation looks like the entropy function of α and β . When the α and β decrease exponentially, m should grow up gradually(sub-exponentially).

Those two important parameters can be obtained in any manners, for instance, we can directly use the historical and statistical data of the ad-hoc network, or use deducible algorithm to predict them.

Following is the framework of our algorithm. The sender algorithm is illustrated in Algorithm 1.

Algorithm 1 Sender's Algorithm Framework

- 1: Every mobile device perform keys exchanging protocol
 - 2: **while** the packet buffer is empty **do**
 - 3: Load a packet from buffer
 - 4: Perform the dispersal part of the IDA algorithm {split the original packet into n packets}
 - 5: Perform m paths selection algorithm
 - 6: Send m pieces packets along the n paths
 - 7: **end while**
-

Remark: Since the sender and receiver should agree to access the same m rows of the matrix D_{mn} . A good choice is the Diffie-Hellman algorithm[7]. There are

also many other approaches can deal with key-exchange problem, we refer to the book[17].

The receiver algorithm is illustrated in Algorithm 2.

Algorithm 2 Receiver's Algorithm Framework

- 1: Let k is the number of packets has received until now
 - 2: **while** $k \leq m$ **do**
 - 3: Receive packets
 - 4: $k = k + 1$
 - 5: **end while**
 - 6: Perform the Reconstruct part of the IDA algorithm to retrieve the original packet from m packets.
-

4.2 Table-Driven Protocol(TDP)

The routing-table framework of sender algorithm is illustrated in Algorithm 3.

Algorithm 3 Table Update Algorithm Framework for TDP

- 1: Periodically Broadcast the routing request
 - 2: Collect all response data from others nodes and construct the routing-tables
 - 3: Whenever update routing-table (the above two steps should be according the original algorithms) perform the decreasing insertion sort According to α, β then stop the sorting till the first m elements are sorted
-

Remark: We can apply our framework to any sorting algorithm, but it could be more time-consuming for instance $O(n \log n)$, where n is the total number of devices of this network. Instead of using other full-sorting algorithms, the alternative is bubble sort.

4.3 On-Demand Protocol(ODP)

The path selection extension algorithm for On-Demand source-initiated algorithm is illustrated in Algorithm 4.

Algorithm 4 Path Selection Extension Algorithm for ODP

- 1: Source broadcasts the routing request
 - 2: Instead of choosing only one path, records the first m paths from the response
-

Remark: Although the algorithm choose the first m path, it does not imply all of them are the shortest path within all response from mid-hops and destination.

Remark: We only focus on the source-initiated algorithm except the zone-based algorithm. We are extending our research to the zone-based algorithms like[10][9].

5 Relationship between Some parameters

In this section, we introduce the powerful tool *Lovász Local Lemma* [2] in the powerful probabilistic method that has found many applications in theoretical computer science. Briefly, given a set of "bad" events in a discrete probability space, the lemma provides a simple inequality which, when satisfied, guarantees that with probability greater than zero, no bad events occurs. The inequality relates the probability that each bad event occurs with the dependence among them. The lemma is nonconstructive, for a discrete probability space, it shows only that there exists some elementary outcome that is not in any bad events.

An event A is mutually independent of a set S if conditioning on whether or not some of the events in S hold does not affect the probability of A . More formally,

$$\text{for every } \mathbb{B}_1, \dots, \mathbb{B}_r, \mathbb{C}_1, \dots, \mathbb{C}_s \in S$$

$$\Pr(A | \mathbb{B}_1 \wedge \dots \wedge \mathbb{B}_r \wedge \overline{\mathbb{C}_1} \wedge \dots \wedge \overline{\mathbb{C}_s}) = \Pr(A)$$

Fact 5.1 (Lovász Local Lemma). Consider a set S of (typically bad) events such that for each $A \in S$

- 1) $\Pr(A) \leq p \leq 1$, and
- 2) A is mutually independent of a set of all but at most k of the other events.

If $4 \cdot p \cdot k \leq 1$ then with positive probability, none of the events in S occur.

Before proceeding, we need to introduce some notations. Let n be the number of parts into which the IDA algorithm wants to disperse the original information, and m be the number among the n pieces which suffice to reconstruct the original information. A P_d is the probability that some path i intersects with other path j , $1 \leq j \leq n, j \neq i$. Let P_f be the probability that any path i , $1 \leq i \leq n$, fails to send some piece into the destination.

We can determinate the m from $\frac{B_w}{B'_w}$ where B_w is the required bandwidth for the client and B'_w is the amortized bandwidth of n servers.

Theorem 5.2. If the first part of the IDA's algorithm attempts to find the mutually independent n paths but some path i intersects with other path j . Let the number of the intersecting paths be up to d . If the value

of P_d ranges from $1/4$ to $\frac{1}{4(n-m)}$, then by Lovász Local Lemma, the IDA-based algorithm can find the m disjoint paths, each path can send data with the bandwidth $\frac{B_w}{m}$.

Proof. By definition, d is the number of possible dependent paths. $\therefore 1 \leq d \leq n$. Furthermore, these m paths that are satisfied with bandwidth $\frac{B_w}{m}$ by sending data should not be intersected with other paths. Otherwise, it is not capable to provide the required bandwidth for client, therefore, $1 \leq d \leq n - m$. Then we want to satisfy the sufficient condition of the Lovász Local lemma, $4 \cdot P_d \cdot d \leq 1$. We can get

$$\frac{1}{4(n-m)} \leq P_d \leq \frac{1}{4}$$

□

Before we begin to relate n with P_d and P_f , we introduce the powerful inequality: Chernoff Bound (another form) [6].

Fact 5.3. *The Chernoff Bound (Another Form)*

Suppose that $x_1, \dots, x_n$ are the independent random variables taking the values 1 and 0 with probabilities p and $1-p$, respectively, consider their sum $X = \sum_{i=1}^n x_i$.

Then for all $0 \leq \theta \leq 1$, $\text{prob}[X \leq (1-\theta)pn] \leq e^{-\frac{\theta^2}{2}pn}$ [6].

Theorem 5.4. *If the IDA-based algorithm intends to route data packets to destination with high probability by using at least m paths, the probability of link failure P_f can be larger $1 - \frac{1 - \frac{1}{4P_d n}}{1 - \theta} \geq 0$.*

Proof. Let $y_1, \dots, y_n$ be the independent random variables for path i , $1 \leq i \leq n$, indicating the values 1 as good link and 0 as bad link with probability $1 - P_f$ and P_f . Then Y is their sum $\sum_{i=1}^n y_i$. If we want to show the data can route to the client with high probability by using at least m paths, that is, we should show the good event that less than m paths are good link is exponentially small. By showing the case we mean here, we must bound the bad event as

$$\text{Prob}[Y \leq m] \leq e^{-\frac{\theta^2 P_f \cdot n}{2}},$$

that is, we satisfy the sufficient condition of

$$(1 - P_f) \cdot n(1 - \theta) \leq m,$$

By the previous result, we can get the inequality

$$m \leq n - \frac{1}{4P_d},$$

Finally, we can show the following

$$1 - P_f \leq \frac{n - \frac{1}{4P_d}}{n - n\theta} = \frac{1 - \frac{1}{4P_d n}}{1 - \theta}.$$

□

Corollary 5.5. *If*

$$m \leq n - \frac{1}{4P_d}$$

then

$$n \geq \frac{1}{4P_d(P_f + \theta - \theta \cdot P_f)}.$$

Proof. It is easy to derive by the intermediate formula from the previous result, that is,

$$P_f \geq 1 - \frac{1 - \frac{1}{4P_d n}}{1 - \theta} \geq 0,$$

After simplifying it, we have the result

$$n \geq \frac{1}{4P_d(P_f + \theta - \theta \cdot P_f)}.$$

□

It is the first time in this field that showing the relation among P_d and P_f , n while appealing the multi-path routing scheme to deal with the QoS issue in ad-hoc networking. The role of θ is not important here, because it is just the parameter for deciding how far we want to bound the concentration range near the expectation.

6 Conclusions

In this paper, we develop general frameworks of multi-path routing scheme for ad-hoc networks. These frameworks provide the high reliability of routing no matter whether the mobile devices is roaming or not. They can be easily applied to every ad-hoc routing protocol. There are two categories of ad-hoc routing algorithm, on-demand and table-driven. We choose a routing protocol for each to demonstrate that it should be easily applied to any other protocol. We also give the probability method to obtain the reliability of HRRF. The probability that fail to transport packet to destination is exponentially small, so it is very highly reliable than other single-path routing protocols.

Acknowledgement

We thank to Yu-Liang Chang and Chi-Yii Tang for constructive discussion about the ad-hoc routing problem and wireless network.

References

- [1] W. Aiello and T. Leighton. Coding theory, hypercube embeddings, and fault-tolerance. *Proceeding of The Third Annual ACM Symposium on Parallel Algorithms and Architectures*, pages 125–136, July 1991.
- [2] N. Alon and J. Spencer. *The Probabilistic Method*. John Wiley and Sons, 2nd edition, 2000.
- [3] A. Bestavros. IDA-based disk array systems. *AT&T Bell Laboratories 45312-890707-01TM*, July 1989.
- [4] A. Bestavros. SETH : A VLSI Chip for the Real-Time Information dispersal and retrieval for security and fault-tolerance. *Proceeding of 1990 International Conference on Parallel Processing*, 1:457–464, 1990.
- [5] A. Bestavros. AIDA-based Real-Time Fault-Tolerant Broadcast Disks. *Proceeding of 1996 IEEE Real-Time Technology and Applications Symposium*, pages 49–58, 1996.
- [6] H. Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Annals of Mathematical Statistics*, pages 23:493–509, 1952.
- [7] W. Diffie and M. E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, pages 644–654, Nov 1976.
- [8] J. Håstad, T. Leighton, and M. Newman. Fast computation using faulty hypercubes. *Proceeding of The Twenty-First Annual ACM Symposium on Theory of Computing*, pages 251–263, May 1989.
- [9] C.C Hsu and L.P. Chou. QoS Routing for Zone-Based Protocol in Ad-Hoc network. manuscript, 2001.
- [10] M. Joa-Ng and I.T. Lu. A Peer-to-Peer zone-based two-level link state routing for mobile Ad-Hoc Networks. *IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks*, 17(8):1415–1425, Aug 1999.
- [11] D. Johnson and D. Maltz. The Dynamic Source Routing Protocol for Mobile Ad-Hoc Networks. *IETF Draft*, page 49, Oct 1999.
- [12] S.J. Lee and M. Gerla. Split Multi-path Routing with Maximally Disjoint Paths in Ad-Hoc Networks. *Proceeding of 2001 IEEE International Conference on Communication*, pages 3201–3205, 2001.
- [13] Y.D. Lyuu. *Information Dispersal and Parallel Computation*. Cambridge University Press, 1992.
- [14] A. Nasipuri, R. Castañeda, and S.R. Das. Performance of Multi-path Routing for On-Demand Protocols in Mobile Ad-Hoc Networks. *Mobile Networks and Applications*, 6:339–349, 2001.
- [15] F. Preparata. Holographic dispersal and recovery of information. *IEEE Transactions on Information Theory*, pages IT-35(5):1123–1124, Sep 1989.
- [16] M.O. Rabin. Efficient Dispersal of Information for Security. *Journal of ACM*, 36(2):335–348, Apr 1989.
- [17] B. Schneier. *Applied Cryptography*. John Wiley and Sons, 2nd edition, 1996.
- [18] A.S. Tanenbaum. *Computer Networks*. Prentice Hall, 3rd edition, 1996.
- [19] A. Tsirigos and Z.J. Haas. Multi-path routing in the presence of frequent topological changes. *IEEE Communications Magazine*, 39(11):132–138, 2001.
- [20] K. Wu and J. Harms. Performance Study of a Multi-path Routing Method for Wireless Mobile Ad-Hoc Networks. *Proceedings of The Ninth International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems*, pages 99–107, 2001.