Policy Management for BGP Routing Convergence Using Inter-AS Relationship

Sang-Jin Jeong, Chan-Hyun Youn, Tae-Sang Choi, Tae-Soo Jeong, Daniel Lee, and Kyoung-Seon Min

Abstract: **The Internet routing instability, or the rapid fluctuation of network reachability information, is an important problem currently facing the Internet engineering community. High levels of network instability can lead to packet loss, increased network latency, and delayed routing convergence. At the extreme, high levels of routing instability can lead to the loss of internal connectivity in wide-area networks. In this paper, we investigate the variation of domain degree and domain count of the inter-domain network over time by using linear regression model in order to analyze the topology variation of inter-domain network. We also propose an efficient policy management model to reduce the instability in the inter-domain routing system. The proposed model can be used to identify whether a routing policy is adequate to reduce convergence time that is required to return to a normal state when BGP routing instability happens. Experimental analysis shows that the proposed model can be used to set up routing policy in domains for the purpose of minimizing the effects and the propagation of BGP routing instability.**

Index Terms: **AS relationship, BGP, instability, convergence, routing policy.**

I. INTRODUCTION

As the Internet grows, the complexity of the routing system increases, and it is needed to analyze the routing characteristics of the Internet. The main factors that affect the inter-domain routing system can be classified into two types [1]. One is inter-AS topology that describes inter-AS peering relations and the other is route stability that indicates the stability of route. As the instability of route increases, routing system exchanges more routing update massages. This causes the waste of network resource and the performance degradation.

In order to analyze routing behavior in the Internet, we can consider end-to-end routing dynamics performed by Paxon [2]. For routing purposes, the Internet is partitioned into a disjoint set of ASs (Autonomous Systems). Originally, an AS was a collection of routers and hosts unified by running a single IGP (Interior Gateway Protocol). Over time, the notion has evolved to be essentially synonymous with that of administrative domain, in which the routers and hosts are unified by a single administrative authority, and a set of IGPs [3].

Whether the use of BGP will scale to a very large Internet depends on the stability of inter-AS routing. If routes between ASs vary frequently—a phenomenon termed flapping [3]—then the BGP routers will spend a great deal of their time updating their routing tables and propagating the routing changes. Daily statistics concerning routing flapping are available from [4]. It is important to note that unstable inter-AS routing can cause unstable end-to-end routing [5]. The routing instability is informally defined as the rapid change of network reachability and topology information. Instability, also referred to as route flaps, significantly contributes to poor end-to-end network performance and degrades the overall efficiency of the Internet infrastructure [6]. Analyzing the topology of the routing system and the instability of the routing system is important for evaluating network performance between end users or develop new protocol. Since the customers of each network are connected to domains and are provided with various services, the instability of domains can severely affect the performance of their customers.

In this paper, to analyze inter-domain topology variation, we investigate the variation of domain degree and domain count over time by using linear regression model, and verify the variation of inter-domain topology. We propose fast BGP convergence policy model to reduce the propagation of BGP routing instability in the inter-domain network. Our model is based on state automaton, and we verify our model with two years of BGP data. Our proposed model can be used for setting up routing policy in ASs for the purpose of minimizing the effect and the propagation of BGP routing instability.

In Section II, the propagation model of BGP routing instability in inter-AS routing is represented, and in Section III, we propose fast BGP convergence policy model to reduce BGP routing instability and verify the correctness of the suggested model. In Section IV, the experimental analysis is discussed and we evaluate the convergence rate of the proposed model. Finally, in Section V, we conclude the applications of fast BGP convergence policy model.

II. INSTABILITY PROPAGATION IN INTER-AS ROUTING

Govindan and Reddy [1] characterized routing system topology, route stability, and the impact of growth on the routing sys-

Manuscript received July 15, 2001.

S.-J. Jeong and C.-H. Youn are with information and Communications University 58-4, Hwaam-dong, Yuseong-gu, Taejon, Korea, e-mail: sjjeong@icu.ac.kr, chyoun@icu.ac.kr.

T.-S. Choi and T.-S. Jeong are with Electronics and Telecommunications Research Institute 161, Gajeong-dong, Yuseong-gu, Taejon, Korea, e-mail: choits@etri.re.kr, tsjeong@etri.re.kr.

D. Lee is with university of Southern California 3740 McClintock Ave. Los Angeles, CA, e-mail: dclee@usc.edu.

K.-S. Min is with Korea Telecom 463-1, Jeonmin-dong, Yuseong-gu, Taejon, Korea, e-mail: minks@kt.co.kr.

This work was partially funded as part of BK-21, KOSEF-Optical Internet Research Center, and by Ministry of Information and Communications, Korea, as part of 2001-S-013, respectively.

1229-2370/01/$10.00 © 2001 KICS

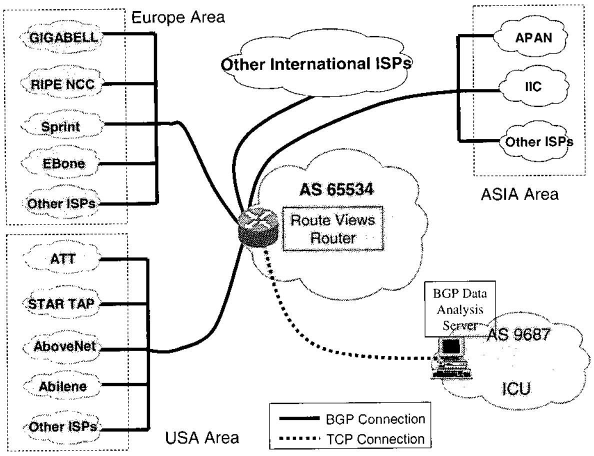


Fig. 1. Network configuration for gathering BGP UPDATE messages.

tem, using two years trace. With collected data, they discovered that inter-AS topology was sparse and that Internet topology could be classified according to domain degrees. According to their analysis, about 87% of domains showed degree less than or equal to 3: stub domains or multi-homed stub domains.

Labovitz *et al.* [5] and [6] examined the network inter-domain routing information exchanged among backbone service providers at the major U.S. public Internet exchange points. They found that the majority of these routing updates are redundant, and they observed several pathological inter-domain routing behaviors. They also identified that most of inter-AS routing information was pathological redundant information. Then, they analyzed the effects of change of the inter-AS routing path on end-to-end customer performance and suggested theoretical computational upper bound and lower bound of inter-AS routing convergence time. Through the experiment, they discovered that the performance of end-to-end user decreased for two minutes after injecting routing information change.

In this section, we discuss topology stability analysis method using BGP UPDATE messages that were collected in the global Internet.

A. Example of Routing Instability Observation

For the analysis, we used BGP UPDATE messages from January 1998 to December 1999 that were collected by Route Views Program operated at University of Oregon [7]. Fig. 1 shows the network configuration for BGP UPDATE messages trace. Data are gathered at every midnight by receiving the whole routing table from BGP peer routers. The Route View Router updates its routing table after receiving routing tables from peer AS's and stores the whole routing table.

In this paper, we classify BGP UPDATE messages into two sets for collected data in 1998 and 1999, respectively.

In general, the domain degree means the number of BGP peerings that the domain has. Therefore, stub domains have mostly degree of 1 or degree of 2; multi-homed stub domains, and domains with a large degree can be referred as backbone domains [8]. Especially, according to the analysis results of Govindan and Reddy [1], a domain with 28 or more degree can be classified as backbone node. As shown in Fig. 2, we can recognize the linear trend of domain degree variation. Moreover, the peaks in the graph imply the rapid change of inter-AS network topology. Much literature did report that these rapid changes were causes of network instability.

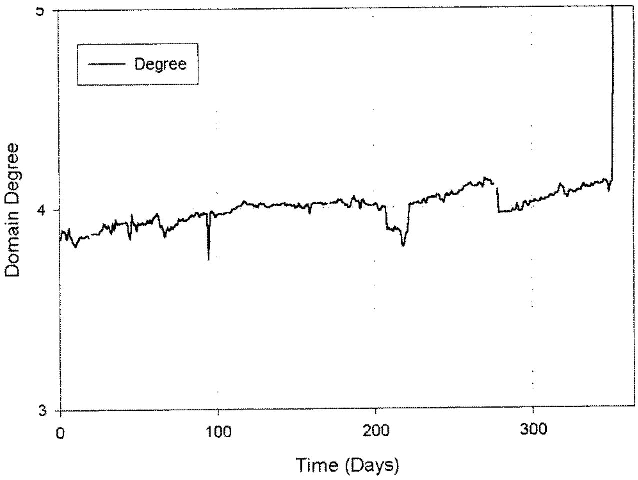


Fig. 2. Day-to-day distribution of domain degree in 1998.

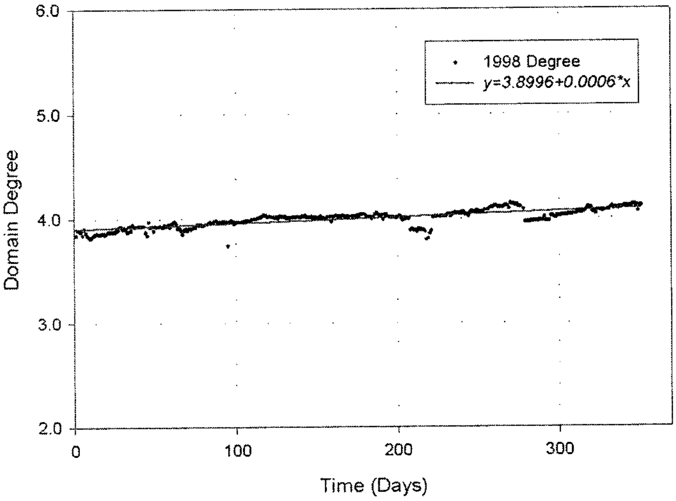


Fig. 3. Regression analysis of day-to-day distribution of domain degree in 1998.

BGP is used to exchange routing information between domains, and it is known that the change of BGP peering topology indicates the change of routing policy or the outage of that domain. Therefore, we can assume that rapid change of domain degree bears direct relation with network instability [3], [9].

Fig. 3 shows the linear regression analysis results to verify the linearity of domain degree variation. We use least square estimation as regression method.

The solid line in Fig. 3 is a result using regression model, and each point represents average domain degree of the whole network for each day. As we can see in the graph, day-to-day distribution of domain degree is well fitted to regression line.

According to the above results, we can conclude that the average domain degree of the network increases linearly in time domain. If we measure the average domain degree of the global network, we can analyze day-to-day distribution of domain de-

Table 1. Internet BGP routing instability report.

Date	AS Number	NAP	BGP Instability (prefix updates)
May 19, 1998	AS3561	AADS	93491 BGP prefix updates
	AS1239	Mae-East	88285 BGP prefix updates
May 20, 1998	AS1239	Mae-East	211037 BGP prefix updates
	AS4058	Mae-West	111957 BGP prefix updates
May 21, 1998	AS3561	AADS	112081 BGP prefix updates
	AS3561	PacBell	69297 BGP prefix updates

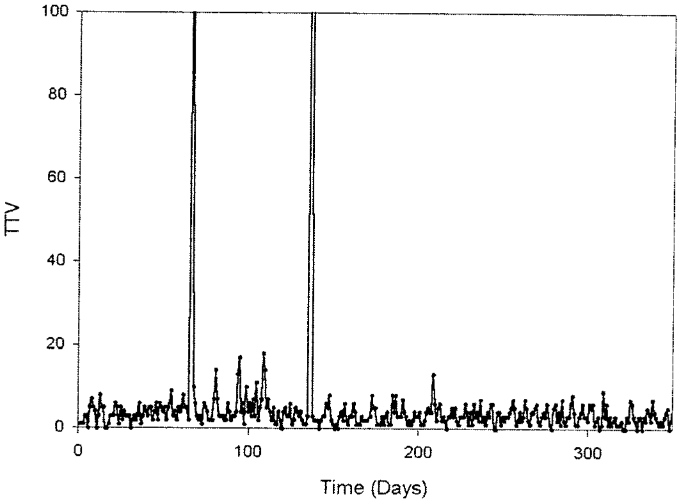


Fig. 4. Temporal topology variation of AS1239.

Table 2. Domain degree of AS1239 around May 20, 1998.

AS Number	Domain degree (TTV)		
	May 19, 1998	May 20, 1998	May 21, 1998
1239	459 (3)	324 (135)	462 (138)

gree based on linear regression model. From Fig. 2, we can observe the rapid decrease of average domain degree of the network, e.g., around 100-th day. Therefore, by the definition of routing instability in Section I, this behavior represents the occurrence of instability. Our proposed model analyzes the propagation behavior of routing instability by identifying the source of routing instability and by using inter-AS relationship.

To identify the source of BGP routing instability in the network, we referred to a report on Internet routing instability that was provided by Merit [4]. Table 1 shows the BGP routing instability around May 20, 1998. From the table, we can see high instability appeared at AS1239 on May 20, 1998, and most BGP instability was contributed by AS1239. Thus, we can suspect that AS1239 is one of the dominant sources that gave rise to BGP instability on that day.

To analyze the instability in AS1239, we compare TTV (Temporal Topology Variation), considering domain degree. TTV denotes absolute value of degree difference between consecutive days. Namely, high value of TTV showing rapid change of topology indicates network instability. Fig. 4 indicates TTV of AS1239. As shown in Table 2, AS1239 shows high value of TTV on May 20, 1998, i.e., 137-th day.

Table 2 summarizes domain degree of AS1239 around May 20, 1998. As appeared in the table, degree of AS1239 was rapidly decreased on that day, and the decrement caused the high value of TTV. Thus, we can see that the sharp peak in Fig. 4 was due to the rapid decrement of domain degree.

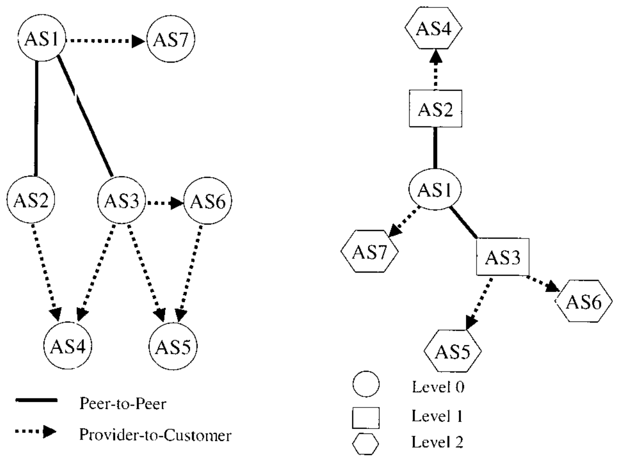


Fig. 5. Level architecture of inter-AS topology.

B. Instability Propagation

Internet routing instability is an important problem currently facing the Internet engineering community. High levels of network instability can lead to packet loss, increased network latency, and time to convergence. In some extreme cases, high levels of routing instability can lead to the loss of internal connectivity in wide-area networks [6]. We investigate the behavior of instability propagation based on inter-AS relationship suggested by Gao [10]. In [10], inter-AS relationship is classified as follows:

Two ASs that exchange traffic have a customer-to-provider, provider-to-customer, peer-to-peer relationship.

- *Customer-to-provider provider-to-customer relationship*: The customer typically belongs to a smaller administrative domain that pays a larger administrative domain for access to the rest of the Internet. The provider is an AS that belongs to the larger administrative domain.
- *Peer-to-peer relationship*: The two peers typically belong to administrative domains of comparable size and find it mutually advantageous to exchange traffic between their respective customers.

To analyze the instability distribution, we use Gao's inter-AS relationship inference algorithms to identify *customer-to-provider and peer-to-peer* relation among ASs. The algorithms, suggested in [10], infer inter-AS relationships from the BGP routing table. Therefore, we extracted AS relationships from `AS_PATH` field in the BGP UPDATE messages by using algorithms in [10]. Fig. 5 depicts the mapping of example inter-AS topology to leveled topology. Inter-AS topology in the side of the figure can be mapped to leveled topology in the right side of the figure. The level of each domain is defined as follows.

Level 0 domain means the source of BGP routing instability. Level 1 domain represents the neighbor having peer-to-peer relationship with level 0. Level 2 domain depicts the neighbor

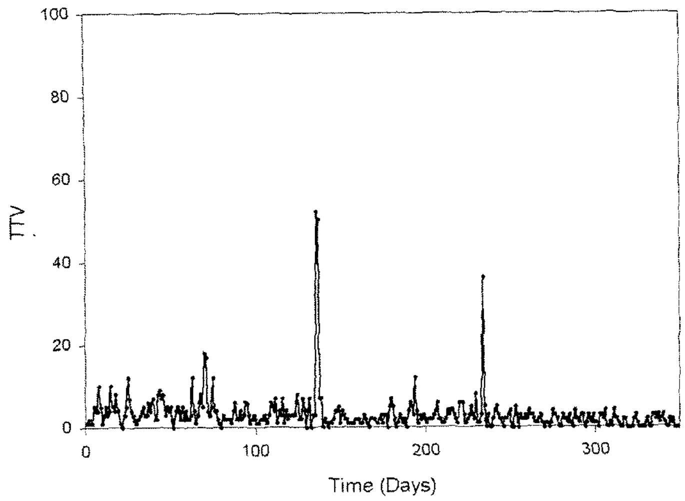


Fig. 6. Temporal topology variation of level 1 AS (AS1).

Table 3. Domain degree of level 1 ASs.

AS Number	Domain degree (TTV)		
	May 19, 1998	May 20, 1998	May 21, 1998
1	205 (3)	153 (52)	201 (48)
701	802 (1)	514 (288)	806 (292)
1673	74 (0)	71 (3)	74 (3)
1740	101 (2)	92 (9)	103 (11)
2548	171 (7)	107 (64)	184 (77)
2914	137 (2)	125 (12)	135 (10)
3561	630 (6)	416 (214)	627 (211)
3847	48 (2)	35 (13)	51 (16)

having customer-to-provider relationship with level 0 or level 1 AS.

The definition of level architecture in inter-AS topology implies that two ASs having peer-to-peer relationship lie in the same level of inter-AS topology, and the customer AS lies in the next level of its provider, except for customers of level 0 AS.

Fig. 6 shows TTV of one AS, namely AS1, neighboring AS1239. AS1 has peer-to-peer relationship with AS1239. According to our analysis, other neighbors of AS 1239 show similar behavior. As we can see in Fig. 6, level 1 AS shows the rapid increment of TTV on 137-th day, (May 20, 1998) same as AS1239. From the figure, we assume that the high instability of certain ASs can be generated by the effect of peer-to-peer relationship between AS pairs.

Table 3 summarizes domain degree of several neighbors ASs of AS1239. These ASs have peer-to-peer relationships with AS1239. Namely, peer-to-peer ASs of AS1239 show rapid domain degree change.

This behavior implies that high BGP routing instability of certain AS can impact on the domain degree of its peer-to-peer AS. Furthermore, with the results of Govindan and Reddy [1], we can classify certain domains as backbone nodes if their degree is over 28, and can understand that domains having peer-to-peer relationship with AS1239 are backbone nodes. Table 4 summarizes the analysis of domain degree distribution of level 1 and level 2 ASs. To analyze degree change of level 2 domains, we select one of peer-to-peer domains of AS1239, then investigate the neighbor ASs of selected domain. In this paper, we choose AS2548 as an origin of level 2 AS. We classify BGP neighbors of AS2548 into peer-to-peer and customer-to-provider AS.

Table 4. Domain degree of level 2 ASs.

Domain Class	Number of domains (%)	Number of domains whose TTV is nonzero (%)	Number of domains whose TTV is zero (%)
Backbone (or Level 1 ASs) (degree≥ 30)	13 (7.6)	12 (92.3)	1 (7.7)
Customer (or Level 2 ASs)	158 (92.4)	92 (58.2)	66 (41.8)

As we can see in the table, 92% of level 1 ASs show the change of TTV, i.e., the change of inter-AS topology, and 58% (or 92 customers) of level 2 ASs show the change of TTV. Since, as shown in the Table 2 and Table 3, the origin of rapid change of TTV on 137-th day is the decrement of domain degree, we can interpret that 58% of level 2 AS experienced the decrement of domain degree on 137-th day in 1998. Furthermore, according to [1], customer (or stub) domains have degree 1 or 2. Therefore, we can understand that the customer domains have lost the connection to their providers, and that the high value of TTV at level 1 ASs was due to the customers. In other words, the topology of backbone nodes having peer-to-peer relationship with each other does not change in the occurrence of BGP routing instability.

III. POLICY MODEL FOR BGP ROUTING CONVERGENCE

In the previous section, we analyzed the topological characteristics of inter-AS topology over time. According to our analysis results in Section II, the topology characteristics of inter-AS network are the linear function. However, we can see the rapid topology change on certain days; e.g., 65-th day, 137-th day in Fig. 4 and so on. Thus, according to the definition of Internet routing instability, we can interpret that instability was generated during those days.

Many research results on the topological characteristics of inter-AS routing system and the origins of Internet routing instability were reported in [1]–[11]. However, there is no work on the propagation of Internet routing instability among domains or the development of systematic model that can represent the propagation of BGP routing instability. In this paper, we analyze the propagation behavior of BGP routing instability by using inter-AS relationships suggested by [10] and propose BGP routing policy model to preserve stability in the inter-AS network during the occurrence of high level instability. It is important to analyze the propagation of instability, because it is possible to set up a routing policy that can efficiently decrease the BGP instability and fast converge to normal state on the basis of the systematic model of instability propagation.

A. Model Description for BGP Convergence Policy

An AS may change the nature of its relationships with its neighbors. For example, a customer may grow large enough

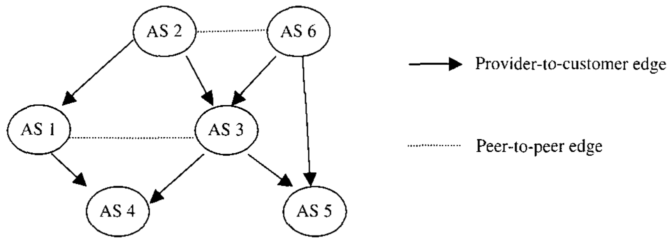


Fig. 7. Example topology showing valley-free relationship.

to renegotiate its relationship with a provider, and the AS pair may make transition into a peer-to-peer relationship. As part of evolving to a new relationship, the two ASs may need to change their import and export policies. Ideally, these changes would occur simultaneously. However, in practice, each AS configures the routers independently of others. As a result, the BGP system can go through a transition period when one AS has changed its configuration and the other has not changed. Since these changes occur on a human time scale, it is important to carefully study the influence of the transition period on system stability. Our proposed model can be used to capture potential convergence problems, and to determine which kind of routing policy should be used to reduce convergence time to normal states from when BGP routing instability happens.

In this section, we discuss fast BGP convergence policy model based on state automaton for reducing the propagation of BGP routing instability and we verify our model with BGP data that are collected in the global Internet. To analyze BGP routing instability propagation, we use AS relationships represented in the following properties that were proposed by Gao [10].

Property 1: The valley-free is defined as follows. After traversing a provider-to-customer or peer-to-peer edge, the AS path can not traverse a customer-to-provider or peer-to-peer edge.

Property 2: If AS path in any BGP routing table entry satisfies valley-free condition, an AS path of a BGP routing table entry has one of the following patterns.

(a) an uphill path,
(b) a downhill path,
(c) an uphill path followed by a downhill path,
(d) an uphill path followed by a peer-to-peer edge,
(e) a peer-to-peer edge followed by a downhill path,
(f) an uphill path followed by a peer-to-peer edge, which is followed by a downhill path.

Here, downhill path is a sequence of edges that are provider-to-customer edges and uphill path is a sequence of edges that are customer-provider edges. For example, in Fig. 7, AS paths (1,2,3) and (1,2,6,3) are valley-free while AS path (1,4,3) is not valley-free.

As proposed by [10], if AS_PATH in a BGP routing information satisfies valley-free condition, it is possible to classify inter-AS topology into peer-to-peer and customer-to-provider relationships.

These relationships translate into rules that determine whether or not an AS exports its best routes to a neighboring AS, e.g., normal export rules [12]. Also, the interaction of locally defined routing policies can have global ramifications for the stability of the BGP system. Conflicting local policies among a collection of ASs can result in BGP route oscillation. To avoid local oscillation, we consider policy model in the theorem.

The safety of a path is defined as follows [11]. An instance of the path is safe if the protocol SPVP (Simple Path Vector Protocol) can never diverge. SPVP is defined in [13].

Theorem 1: If an inter-AS routing policy satisfies property 1 and property 2, there exists a state automaton model to guarantee safety in inter-domain routing.

Proof: Let us assume that AS_PATH field in the BGP routing table satisfies valley-free property and that we can describe inter-AS topology as AS relationships such as peer-to-peer or customer-to-provider. Let us denote parameters to describe inter-AS routing policy as follows:

- i and j denote *originating* and *terminating* nodes, respectively, in a AS_PATH.
- m and n denote *endpoints* of a BGP connection that might occur in AS_PATH.
- Number of nodes in the network is N.
- Number of domain degree is d.
- Inter-AS topology matrix P, where P_{mn} denotes the number of BGP peers interconnection nodes m and n.
- Inter-AS R, where R_{ij} denotes the number of AS_PATH from node i to node j in the inter-AS topology.

We can define the state of network as a tuple (R, P). Changes in the network state occur as the topology matrix P is updated. We assume that the current matrix P completely summarizes the entire history of topology changes. If the topology matrix P changes to a new P', and the optimal inter-AS topology according to P' is R', we should make a decision whether to keep the topology R constant or change it to the new R'. To formulate this decision problem, we need to specify reward and cost functions associated with each transition. Consider a network in state (R, P) that takes a transition to state (R', P'). The network acquires an immediate expected reward equal to $((R', P'), (R, P))$. Also a reconfiguration cost is equal to $(\mathrm{D}(R, R'))$, where $\mathrm{D}(R, R')$ is the distance between R and R', and we assume that R is not equal to R'. The problem is how to prune customer domains in the case of high BGP routing instability so as to maximize the expected reward minus the inter-AS connectivity (i.e., domain degree) over an infinite time horizon. Let $(R^{(k)}, P^{(k)})$ denote the state of the network immediately after the k-th transition, and Z be the set of admissible policies, so the network pruning problem can then be formally stated as to find an optimal policy $z^* \in Z$ that maximizes the expected reward function:

$$F =$$

$$\lim_{k\to\infty} \frac{1}{k} E\{\Sigma_{l=1}^{k} \alpha[R^l, P^l), (Rl^{l-1}, P^l)] - \beta[D(Rl-1), R^l)]. \tag{1}$$

Therefore, we can model inter-AS routing policy as a state automaton with output.$(q.e.d)$ □

B. Policy Management for BGP Routing Convergence

Generally, to make a systematic model about the spread of certain events, state automaton can effectively explain their propagation behavior [14]. Therefore, according to the above theorem, we can make a inter-AS routing instability propagation model using state automaton as a DES (Discrete Event System).

The transition between states happens while traversing inter-AS topology. According to AS relationship between two ASs, there exist at most two possible transitions for each state. The output is generated during state transition. Output indicates the probability of pruning customer's logical connection to provider. The probability has two cases, 0 and p_{tr}. 0 means that the provider will not prune the connection of customer that has customer-to-provider AS relation. p_{tr} represents a probability when the provider will prune connection of customer. Furthermore, while analyzing the state transitions in the automaton, the conceptual model of topology reconfiguration can be used to determine state transition probability, i.e., p_{tr}.

To solve the state transition, we consider a state automaton with output$(E, X, \Gamma, f, x_o, Y, g)$; each parameter is formulated as shown.

A set of events E consist of two events α and β.α means that neighbor AS is peer-to-peer relationship and β means that neighbor AS is customer-to-provider relationship. A set of states X has three entities, p_s, p, and c, which represent starting state, current state that has peer-to-peer relationship with previous state, and current state that has customer-to-provider relationship with previous state, respectively. A set of feasible events Γ can be formulated as follows.

$$\Gamma(P_s) = \Gamma(C) = \{\alpha, \beta\} \tag{2}$$

$$\Gamma(P) = \{\alpha\} \tag{3}$$

Let state transition function f^X be represented as follows.

$$f^X(P_s, \alpha) = f^X(C, \alpha) = p \tag{4}$$

$$f^X(P_s, \beta) = f^X(C, \beta) = f^X(P, \beta) = C \tag{5}$$

The set of outputs Y has two entities. The output function g maps the pair of the set of states X and the set of events E to the set of outputs Y. Formal definition is given as follows.

$$g^X(P_s, \alpha) = g^X(C, \alpha) = 0 \tag{6}$$

$$g^X(P_s, \beta) = g^X(C, \beta) = g^X(P, \beta) = P_{tr} \tag{7}$$

Finally, the initial state x_0 represents the source of BGP routing instability, namely p_s . Thus, the state diagram of proposed state automaton is depicted in Fig. 8. In the Figure, the state transition $(\alpha, 0)$ implies that an AS sends all BGP UPDATE messages to its neighbor in peer-to-peer relationship. Generally, ASs in peer-to-peer relationship are backbone nodes, so it is more important to keep knowing the status of the global Internet. However, in the case of customer-to-provider relationship, i.e., state transition (β, p_{tr}), customer AS is comparably small size, so a provider AS sends some of BGP UPDATE messages to its customers in the case of high routing instability. By this behavior, a provider can regulate the propagation of routing instability to customers, i.e., ASs in customer-to-provider relationship.

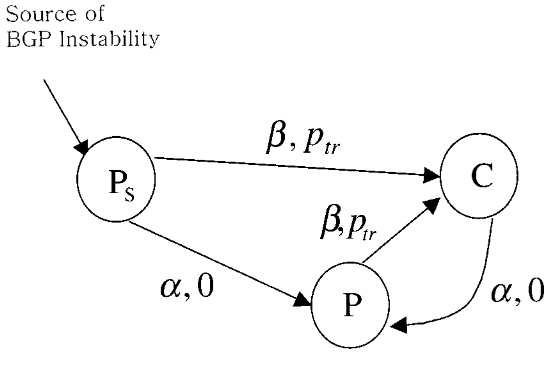


Fig. 8. State automaton model for inter-AS routing policy.

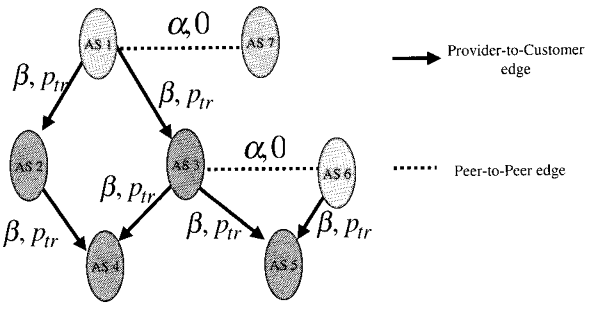


Fig. 9. Example of BGP routing instability propagation.

As proposed in [15], the state transition probability p_{tr} can be determined by statistical analysis of large number of samples using inter-AS relationships. Fig. 9 shows the application of our proposed model. Let AS 1 be the source of BGP routing instability. As the instability propagates from AS 1 to its neighbors, each AS sets its routing policy, z, according to the AS relationship with its neighbor.

In the above example, AS1 has one peer-to-peer AS (AS7) and two provider-to-customer ASs (AS2 and AS3). Since AS1 has peer-to-peer relationship with AS7, AS1 does not make a change in the edge for AS7. But in case of AS2 and AS3, the edge is provider-to-customer, so AS1 (provider AS) sets its routing policy to cut its customers according to the probability P_{tr}. Therefore, by pruning its customers, AS1 can prevent customers from transmitting their traffic toward AS1, can fast recover from high instability and can control the propagation range of the instability. Moreover, by choosing optimal P_{tr}, the BGP routing instability propagation range can be adjusted.

In order to discuss the routing convergence of the proposed model, we assume the following.

Assumption 1: 1) We assume that inter-domain topology

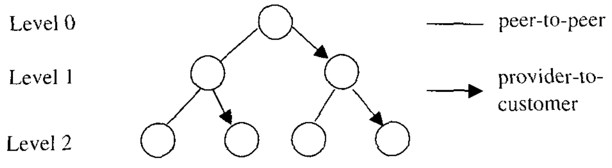


Fig. 10. Two level inter-AS topology.

shows two types of inter-AS relationships, e.g., peer-to-peer and provider-to-customer.

2) We assume the probability of occurrence of each inter-AS relationship is equally distributed.

Routing policy that following the proposed model converges the BGP routing instability propagation in inter-AS network. Moreover, the convergence rate can be restricted by the following Theorem 2.

Theorem 2: If the propagation of routing instability follows the Assumption 1, the event probability for fast convergence policy is restricted by the following equation.

$$P(convergence\ within\ Level\ n\ domain) = 1 - \frac{(2-p_{tr})^n}{2^n}$$

where n is domain level and P_{tr} is given.

Proof: Since there exists two types of inter-AS relationships and each relationship can occur in equal probability, there are 2^n of routing paths according to the classification of inter-AS relationships from Level 0 domain to Level n domain. Fig. 10 shows an example of two level topology.

In our proposed model, the network topology that is made up of peer-to-peer relationship does not change in the occurrence of routing instability.

From Fig. 10, we can see that there are four kinds of routing paths and the probability of instability propagation is computed as follows.

Peer-to-peer → peer-to-peer : $1*1$
Peer-to-peer → provider-to-customer : $1*(1-P_{tr})$
Provider-to-customer → peer-to-peer : $(1-P_{tr})*1$
Provider-to-customer → provider-to-customer : $(1-P_{tr})*(1-P_{tr})$.

Then, by using $1-P_{tr}$, average probability of routing instability propagation from Level 0 domain to Level n domain can be shown as

$$P = \frac{\sum(1-p_{tr}) for\ each\ path}{Total\ number\ of\ paths}. \tag{8}$$

Since the denominator of (8) is 2^n in level n domain and the numerator can be represented as $(2-P^n_{tr})$ according to the binomial distribution, average probability of inst-ability propagation is equal to

$$\frac{(2-p_{tr})^n}{2^n}.$$

Also, the convergence probability is equal to

$$1 - \frac{(2-p_{tr})^n}{2^n}.$$

Therefore, our proposed model converges to nominal state as domain level increases. Furthermore, there exists a routing policy that can stabilize the BGP routing instability.$(q.e.d)$ □

Table 5. Probability of p_{tr} : level 0 → level 1.

Domain Class	Number of domains (%)	Number of domains whose TTV is nonzero (%)	Number of domains whose TTV is zero (%)
Backbone (degree ≥ 30)	23 (5.1)	21 (91.3)	2 (8.7)
Customer	430 (94.9)	207 (48.1)	223 (51.9)

Table 6. Probability of p_{tr} : level 1 → level 2.

Domain Class	Number of domains (%)	Number of domains whose TTV is nonzero (%)	Number of domains whose TTV is zero (%)
Backbone (degree ≥ 30)	13 (7.6)	12 (92.3)	1 (7.7)
Customer	158 (92.4)	92 (58.2)	66 (41.8)

IV. EXPERIMENTAL ANALYSIS OF PROPOSED MODEL

Since it is important to evaluate the convergence rate of proposed model and its the applicability to real inter-AS network, in this section, we investigate the convergence rate of our proposed model with two years data. According to [15], the state transition probability of the proposed automaton can be determined by statistical analysis of large number of samples.

Fig. 11 shows the analysis procedure of BGP routing instability. At first, let us assume that high BGP routing instability arises from AS1239 because of the misconfiguration of its routing policy. Since we already analyzed that AS1239 was the source of high level BGP routing instability on May 20, 1998 and the origin of instability was AS discrepancy with IRR, so this assumption is reasonable. From AS1239, we analyze peer-to-peer ASs with AS1239, because AS1239 is a major IXP in the Internet and as proposed by [5], it is important to analyze the routing behavior of backbone nodes. Furthermore, the peer-to-peer ASs of AS1239 have domain degree greater than 30 and by [1], it is possible to classify theses ASs into backbone nodes.

In the Figure, AS1239 is BGP routing instability source and is defined as level 0. Then we compute the probability of customer pruning by statistical analysis. For example, according to our analysis results, there were 158 Level 2 customers of level 1, AS2548, before BGP routing instability and 92 level 1 customers were pruned by AS2548 during the high level BGP routing instability. So we can compute that the probability of customer pruning level 2 ASs is 0.58. Table 5 and Table 6 show the probability of customer pruning.

Therefore, provider AS can determine the routing policy, according to our proposed model during BGP routing instability at high level, to keep its connection to global Internet by pruning its customers with probability p_{tr}.

The convergence rate of our proposed model can be computed as follows. Let p_1 and p_2 be p_{tr} of level 1 customers

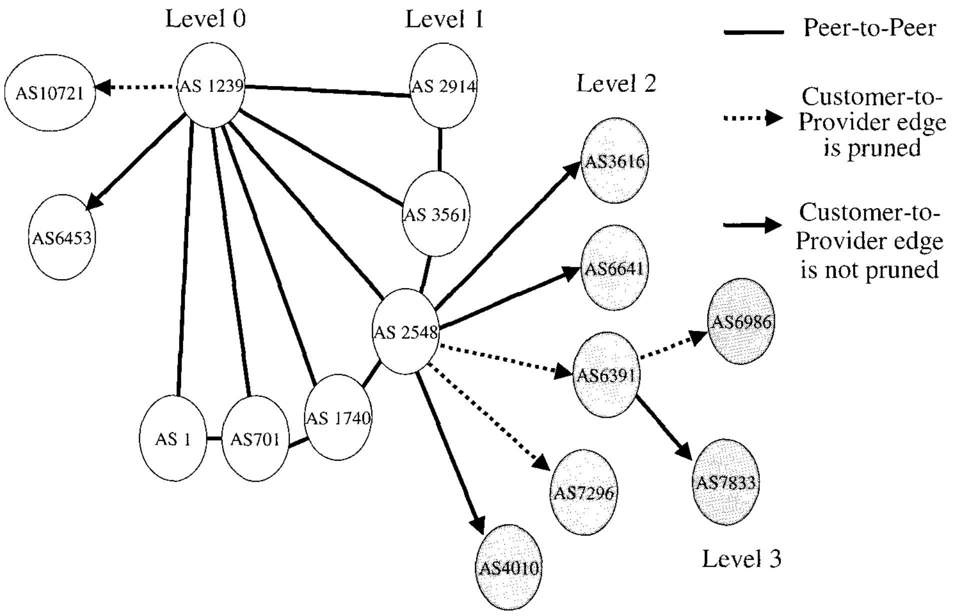


Fig. 11. Experimental analysis of inter-AS convergence model.

and p_{tr} of level 2 customers respectively. Since p_{tr} implies that the probability of BGP routing instability can be absorbed in that level, the probability that BGP routing instability is not absorbed within level 2 domains is $1-(1-P_1)*(1-P_2)$. In our analysis the convergence rate shows 0.783. As we proposed in Theorem 2, if we consider the probability p_{tr} as 0.532, which is the mean value of P_1 and P_2, we can get about 77% of convergence rate within level 2 domains. Therefore, it is possible to reduce routing instability by using routing policy according to our proposed model.

The applicability of proposed model can be summarized as follows: When BGP routing instability happens, by pruning some of customer connections, backbone domains reduce incoming customer traffic. Thus, backbone topology can be preserved, although BGP routing instability occurs. We can interpret this behavior as a routing policy for the purpose of fast recovery of backbone domains during the occurrence of BGP routing instability. In inter-AS routing system, to preserve reliability of network, it is possible to guarantee routing path between peer-to-peer ASs. Moreover, it is important to keep redundancy or available routing path in inter-AS topology.

V. CONCLUSIONS

Internet routing instability is an important problem currently facing the Internet engineering community. It is known that high levels of network instability can lead to packet loss, increased network latency and time to convergence. In some extreme cases, high levels of routing instability can lead to the loss of internal connectivity in wide-area networks. However, there are few works related to the propagation of the instability in inter-AS network and the routing policy that can preserve the reliability during the occurrence of high level instability.

In this paper, we analyzed the variation of domain degree and its count over time by using linear regression model and verified the variation of inter-domain topology to analyze inter-domain topology variation. We also proposed policy model for fast BGP routing convergence policy model to reduce the effects of BGP routing instability. The proposed model is based on state automaton derived from border router's behaviors and we verified it through the analysis of BGP data gathered in major IXPs in the Internet. We also investigated the convergence rate of our proposed model and showed that the convergence rate of instability within level 2 ASs is about 78%. Therefore, we conclude that the proposed model can be used to identify potential convergence problems and to determine which kind of routing policy is adequate to reduce transition period when BGP routing instability or network configuration change happens. Moreover, we showed it is possible to reduce routing instability by using routing policy with considerations of inter-AS relationship.

Namely, our proposed model can be used to set up routing policy in autonomous system for the purpose of minimizing the effect and the propagation of BGP routing instability.

REFERENCES

[1] R. Govindan, A. Reddy, "An analysis of internet inter-domain topology and route stability," in *Proc. IEEE INFOCOM*, 1997, pp. 850–857.
[2] Vern Paxon, "End-to-end routing behavior in the internet," in *Proc. ACM SIGCOMM*, Sept. 1997.
[3] Bassam Halabi, *Internet Routing Architectures*, Cisco Press, 1997.
[4] Available at http://www.merit.edu/.
[5] C. Labovitz *et al.*, "Delayed internet routing convergence," in *Proc. ACM SIGCOMM*, Aug. 2000.
[6] C. Labovitz, R. Malan, and F. Jahanian, "Internet routing instability," in *Proc. ACM SIGCOMM*, Sept. 1997.
[7] Available at http://www.antc.uoregon.edu/route-views/.

[8] S.-J. Jeong and C.-H . Youn, "An analysis of routing instability based on internet topology," in *Proc. ICEIC*, Aug. 2000.

[9] Y. Rekhter, "A border gateway protocol 4," Request for Comments, 1771, IETF, Mar., 1995.

[10] L. Gao, "On inferring autonomous system relationships in the internet," in *Proc. IEEE GLOBECOM*, Nov. 2000.

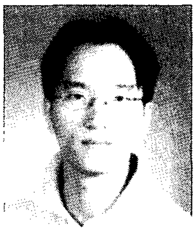
[11] L. Gao and J. Rexford, "Stable internet routing without global coordination," in *Proc. ACM SIGMETRICS*, June 2000.

[12] C. Alaettinoglu, "Scalable router configuration for the internet," in *Proc. IEEE IC3N*, Oct. 1996.

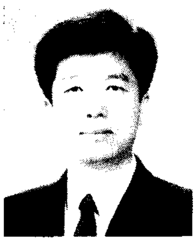
[13] T. G. Griffin and G. Wilfong, "A safety path vector protocol," in *Proc. IEEE INFOCOM*, Mar. 2000.

[14] C. G. Cassandras, "Discrete event systems," Aksen Associates, 1993.

[15] I. Baldine and G .N. Roushas, "Traffic adaptive WDM networks : A study of reconfiguration issues," *J. of Lightwave Technol.*, vol. 19, no. 4, Apr. 2001.

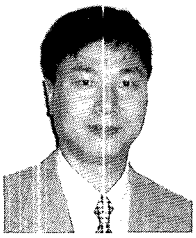


Sang-Jin Jeong received his M.S. (2001) from Information and Communications University, Korea in Communications, B.S. (1999) from Korea Advanced Institute of Science and Technology (KAIST) in Computer Science. During 1999, he served at Korea Telecom (KT) Traffic Engineering Research Laboratories as an invited researcher and he served at University of Southern California, Dept. of Electrical Engineering as a visiting scholar in 2001. Since 2001, he has been enrolled as a Ph.D. candidate at Information and Communications University, Korea. His current interests include Grid middleware, routing stability, and network performance measurement.

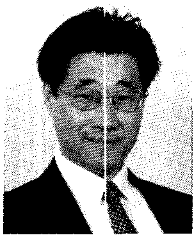


Chan-Hyun Youn received BS and MS degrees in Electronics Engineering from Kyungpook National University, Taegu, Korea, in 1981 and 1985, respectively. He also received a Ph.D. in Electrical and Communications Engineering from Tohoku University, Japan, in 1994. He served at Korean Army as a communications officer, First Lieutenant, from 1981 to 1983. Before joining the University, from 1986 to 1997, he was a leader of high-speed networking team at Korea Telecom (KT) Telecommunications Network Research Laboratories. Where he had been involved in the research and developments of switching system maintenance system, high-speed networking, and HAN/B-ISDN network testbed. Especially, he was a principal investigator of high-speed networking projects including ATM technical trial between KT and KDD, Japan, Asia-Pacific Information Infrastructure (APII) testbed, KOREN and APAN, respectively. Since 1997, he has been an associate professor at Information and Communications University, Taejon, Korea. He also is a chair of resource management and scheduling WG in Grid Forum Korea. Currently, he is interested in the Grid middleware, high performance routing, multicasting, optical Internet, and network performance measurement. He was a recipient of IEICE PAACS friendship prize, Japan, in 1994.

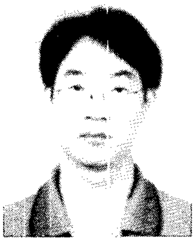
Tae-Sang Choi received his Ph. D. degree from University of Missouri-Kansas City, in 1995. From 1996 to 1998, he served at Multimedia Communications Team in ETRI. Since 1999, he has served at Internet Architecture Team in ETRI. His current research interests include QoS Management and Traffic Engineering in IP Networks, Interactive Multimedia Service System, and Network, System, and Service Management.



Tae-Soo Jeong received his M.S. degree from Kyungbook National University in 1983. He has served at Internet Architecture Team in ETRI since 1983. His research interests include Internet & Data Networks, Telecommunication Systems, and Network Management.



Daniel Lee received his Ph.D. (1992) and S.M. (1987) both from the Massachusetts Institute of Technology in Electrical Engineering and Computer Science, B.S. (1985) in Electrical Engineering with Honors, and B.S. (1985) in Mathematics from the University of Maryland. His Ph.D. thesis published in 1992 at MIT and subsequent publications address various aspects of network modeling, performance analysis, control, and management. From 1993 to 1998, Dr. Lee was devoted to network systems engineering in the U.S. Naval Research Laboratory (NRL), Washington, DC. At the Center for Computational Science in NRL, Dr. Lee participated in the development of the object–oriented protocol software framework, CASiNO (Component Architecture for Simulating Network Objects), and network signaling simulators, SEAN (Signaling Entity for ATM Networks) and PRouST (PNNI Routing Simulation Toolkit). At the Naval Space Center in NRL, Dr. Lee developed a proxy agent that allows the inter-operation of commercial standard network management system and the network management modules of the U.S. government's information collection and dissemination system, ICEbox. In addition to such development activities, Dr. Lee dedicated most of his time to the network modeling and simulation for improving the reliability, availability, maintainability, operability, and security of the information collection and dissemination systems. In 1998, Dr. Lee joined the Electrical Engineering Department of the University of Southern California and has been continuing the network research. His current interests include quality of service of wireless, WDM, and the next-generation internet. Dr. Lee's honors include: 1995 Alan Berman Research Publication Award from NRL, 1995 Navy's Outstanding Performance Award in NRL, and 1989 Teaching Award from MIT.



Kyoung-Seon Min received his B.S in electronic engineering from Korea University and M.S in computer science from Hanyang University, Korea, in 1980 and 1991, respectively, and Ph.D. degree in electronic engineering from Aju University, Korea, in 1997. In 1980, he joined ETRI, where he worked on the design of MTIP(Magnetic Tape Interface Processor). In 1984, he moved to Korea Telecom, where he worked on the development project for TDX-1/1A/1B/10 switching system during 1984 to 1993. From 1994 to 1996, he has been in charge of designing and developing ATM switching system. He is currently working on optical internet project and NOC (Network Operation Center) for KOREN(Korea Research and Education Network). His research interests include optical internet and GMPLS, optical ethernet, and optical switching.