Detection and Diagnosis of Inter-AS Routing Anomalies by Cooperative Intelligent Agents

Osamu Akashi[1], Atsushi Terauchi[1], Kensuke Fukuda[1], Toshio Hirotsu[2], Mitsuru Maruyama[1], and Toshiharu Sugawara[3]

[1] NTT Network Innovation Labs., 3-9-11 Musashino-shi, Tokyo 180-8585, Japan
{akashi,terauchi,fukuda,mitsuru}@core.ecl.net
[2] Toyohashi University of Technology, Aichi, Japan, hirotsu@ics.tut.ac.jp
[3] NTT Communication Science Labs., Kyoto, Japan, sugawara@core.ecl.net

Abstract. Verifying whether the routing information originating from an AS is being correctly distributed throughout the Internet is important for stable inter-AS routing operation. However, the global behavior of routing information is difficult to understand because it changes spatially and temporally. Thus, rapid detection of inter-AS routing failures and diagnosis of their causes are also difficult. We have developed a multi-agent-based diagnostic system, ENCORE, to cope with these problems, and improved its functions (ENCORE-2) through our experience in applying the system to commercial ISPs. Cooperative actions among ENCORE-2 agents provide efficient methods for collecting, integrating, and analyzing routing information observed in multiple ASes to detect and diagnose anomalies that human operators have difficulty in handling. ENCORE-2 is also applied to the hijacked route problem, which is one of recent major inter-AS issues.

1 Introduction

The Internet currently consists of more than 15000 ASes (autonomous systems), and this number is still increasing. Inter-AS routing controlled by BGP-4 [1], however, is not stable [2]. Various analyses of this routing behavior and causes of routing instability have been reported [3]. An essential problem is the difficulty of understanding the spread of routing information advertised by an AS [4]. Unlike intra-AS anomalies, the causes of inter-AS anomalies typically exist outside network operator's domain, while the effects of anomalies are sometimes observed only in the advertising AS. This situation is illustrated in Fig. 1. AS_{self} can see the routing information advertised by AS_x and forward packets to AS_x accordingly. On the other hand, packets directed to AS_{self} from AS_x are forwarded according to the routing information advertised from AS_{self}. In this case, AS_{self} has difficulty determining whether its routing information has reached AS_x or was discarded at an intermediate AS where some filter was applied. The operators of an intermediate AS have difficulty detecting this anomaly because incoming and outgoing packets concerning the intermediate AS are not affected

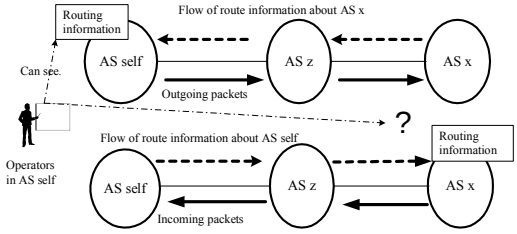

Fig. 1. Problem of verifying spread of routing information

by the filter. Thus, information from other observation points is needed to diagnose this kind of anomaly.

The difficulty of inter-AS routing management comes from noncentralized and autonomous operations. ASes dynamically change their routing relationships with respect to each other. Such temporal changes require on-demand verification and thus invalidate any analysis done in advance. For example, declarative data about each AS's relationships with neighboring ASes are stored in the Internet Routing Registry (IRR) [5], but these data do not necessarily reflect the current statuses of all ASes [6]. Therefore, the data cannot be directly applicable to reachability verification. Moreover, accurate detection of anomalies requires statistical analysis to extract local trends from continuously observed routing information at each observation point. The statistical data, such as the average number or range of BGP full-routes, are required to isolate an anomalous state from a normal one with greater probability. These data are also used to determine when to invoke diagnostic actions.

Centralized analytical approaches [3], some of which use BGP update data collected from multiple ASes, have been proposed, but the autonomy and dynamics of the Internet make performing their analysis difficult and all possible cases are not covered. A method using a cooperative distributed solution (CDS) coincides with this control structure and supplements these other analytical methods. In addition to handling the autonomy of each AS, a CDS would have several advantages over the centralized system approach. From the viewpoint of diagnostic systems, a CDS can be efficient and scalable because 1) statistical calculation to extract local trends in traffic or routing information is performed at the observation points; and 2) the distributed entities, *agents*, exchange only abstracted, analyzed results, rather than raw data. A simple repeated query-and-reply scheme produces a lot of traffic. From the viewpoint of diagnostic functions, a CDS offers higher availability because an agent can act even under the condition where some paths on certain IP networks are unreachable. Agents can try to communicate with each other by relaying messages through a number of cooperative agents. Moreover, a CDS can perform effective analysis because an agent can request other agents to invoke various sensing tools, such as `traceroute` or `ping`, to obtain the remote data and accurately isolate causes of problems. Centralized approaches are, however, incapable of performing these actions at remote points.

To achieve rapid detection and real-time diagnosis of inter-AS routing anomalies, we first analyzed a few years of BGP-related troubleshooting records in our AS to determine the basic functions required for an inter-AS diagnostic system. Then, we designed and implemented a multi-agent-based diagnostic system, called ENCORE [4], which has been applied in actual networks including those of major commercial ISPs for several years and is currently used in commercial operation [7]. The next generation of ENCORE (ENCORE-2) has now developed based on this experience, in order to adapt to recent changes in inter-AS problems. A previous paper [4] described ENCORE's basic diagnostic model and agent architecture, and gave some application examples. This paper focuses on the diagnostic functions of ENCORE-2, which have been extended based on our experience: data collection by agents at multiple observation points, finding indications of anomalies, and analyzing their causes, including the problem of how to handle the hijacked route problem, which is one of recent major inter-AS issues [8]. Anomalies caused by this kind of advertisement were observed a few times a year and were serious problems for commercial ISPs.

2 Analysis of Inter-AS Anomalies

2.1 Difficulties in Inter-AS Routing Management

The difficulties in understanding inter-AS routing can be summarized as follows.

1. [**Spatial changes**] The routing information is physically and geographically distributed and may vary depending on the observation points.
2. [**Temporal changes**] The routing information changes over time.
3. [**Administrative domain**] Routing is controlled independently by each AS. Any operators in other ASes cannot directly access these routing data.
4. [**Local trend**] Each observation point has its own local trends in the dynamics of routing information. Information about these trends can be acquired only through actual observation at each point and statistical analysis of the observed data.
5. [**Limitation of human operators**] Detection and diagnosis require human operators to repeatedly observe and analyze large amounts of routing information, including raw data such as BGP update messages. They also require operators to have sophisticated expertise on where and how to collect and analyze data.

The spatial changes easily lead to inconsistent routing states among several ASes, even though each AS is working consistently with respect to neighbor ASes. Moreover, the ASes experiencing anomalies may be different from those causing the anomalies. Therefore, we need to obtain a global view of routing information to verify whether advertised routing information is spreading as the originating AS intends. The temporal changes make advance analysis invalid. Overcoming this problem requires verification at multiple observation points on an on-demand basis. Operators can use tools such as `ping`, `traceroute`, and `looking glass` [9], but they have to use these tools repeatedly over a long period to confirm their own AS's advertisement and find an anomaly as soon as possible.

Table 1. Categories of BGP-related anomalies

category	rate
R1: Received-policy (local)	19%
R2: Received-others (local)	9%
B: Border-area	15%
A1: Advertised (remote)	42%
A2: Advertised-complicated	15%

2.2 Taxonomy of Anomalies

The results of our analysis of BGP-related troubleshooting records from our AS are summarized in Table 1. 28% of the records, denoted *R1* and *R2*, concern received BGP information. *R1* is the set of anomalies caused by erroneous operations when applying our AS's policy by adjusting the attribute values of received BGP information. *R2* is the set of anomalies whose causes do not directly concern BGP, but concern local errors that indirectly affect BGP control. For example, the loss of reachability to the `next_hop` IP address caused by an IGP configuration error belongs to *R2*. No collaborative analysis with other ASes is required because these two groups of anomalies can be locally analyzed.

The remaining 72% of the records cannot be analyzed without BGP information obtained from outside the AS. These records therefore require inter-AS coordination. The third category *B* involves anomalies that occurred in the area bordering the neighbor ASes. Analysis of anomalies in *B* requires status data about the border area such as the connection status of BGP processes and the IP reachability status in the segment used for BGP peering. A part of the data can be observed from the local AS. Their further analysis, however, often requires information observed from neighboring ASes. The *A1* and *A2* categories of anomalies occurred in remote ASes and have almost the same features. They are distinguished by the types of collaborative actions. *A1* accounts for more than 40% of the records and is the set of anomalies that required confirmation in a simple Q&A fashion between the local AS and remote major transit ASes. These anomalies typically occurred after some modification due to configuration changes or maintenance work. Another 15% of the records, which are categorized in *A2*, can also be handled by inter-AS cooperation, but they require more sophisticated actions to analyze the anomalies than those for *A1*. Such actions would include execution of sensing tools from other ASes after exchanging observation results. In some cases, these actions would require changes in cooperative agents to obtain more suitable observation points.

3 Multi-agent-based Diagnosis

3.1 Required Cooperative Functions

According to the analysis in section 2, a global view of the current routing information that has spread among different administrative domains is essential

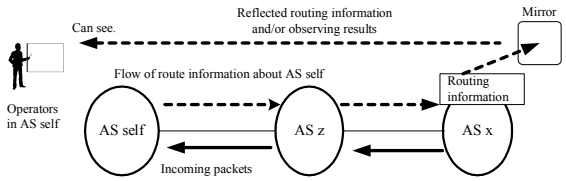

Fig. 2. Reflector model: basic idea for observing spread of information

for diagnosing inter-AS routing anomalies. Since complete understanding of the global view is impossible, we adopt the use of routing information observed almost simultaneously at multiple ASes. By integrating these observed results, we can infer a part of the global view for the purpose of diagnosis. To achieve these coordinated actions, we have proposed a diagnostic system called ENCORE that adopts a multi-agent architecture and utilizes cooperative actions to resolve problems described in section 2.

The basic idea of this system is the reflector model as illustrated in Fig. 2. The essence of this model is to provide a function by which an agent can request a remote agent to observe routing information about a specific AS, which is usually the AS of the requesting agent. The routing information observed and analyzed by remote agents is sent to the requesting agent. Although the reflector model can provide a cooperative function, this function should be performed on an on-demand basis. Thus, a function that enables an agent to request a remote agent to continuously observe the routing information of a specified AS and to notify the requesting agent when specified events occur is required for efficient verification and rapid detection. For example, if the remote agent finds a change in the origin AS number of the BGP attribute value of a specified IP address, it notifies the requesting agent of this observed change. This function is effective because the remote ASes receiving routing information usually become aware of failures earlier than the originating AS.

Another useful function enables the relay of messages to appropriate agents. The relay function is necessary to cooperatively deliver important messages to destination agents even when direct IP routes for message delivery become unavailable. This function is achieved by having the agents act as application gateways. This function is useful because 1) the system can use paths that are not used in usual IP routing, and these paths can include non-transit ASes; and 2) messages whose source IP addresses have changed can pass misconfigured filters with a high probability. Message loops and a significant increase in the number of copied messages are prevented by utilizing information about the path that a message has traversed and restricting the maximum number of hops over which a message can be delivered. When failures are caused by filter setting errors, which are typical configuration mistakes, exchanging messages at the end-to-end level is sometimes impossible. In the case of Fig. 2, if an intermediate AS filters routing information advertised from AS_{self}, AS_{self} cannot access AS_x to verify reachability. In this situation, AS_{self} can exchange messages with AS_x

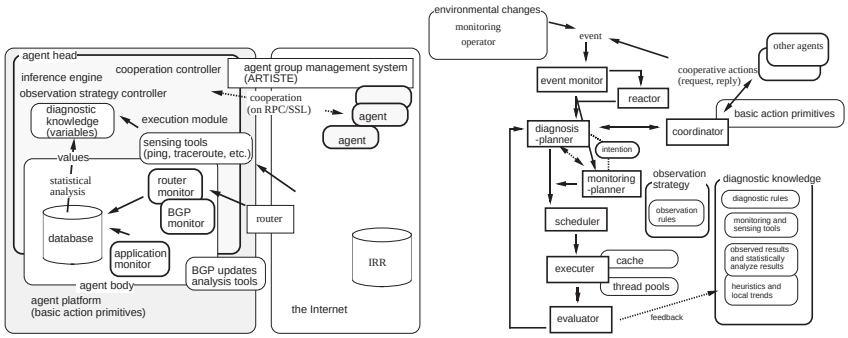

Fig. 3. ENCORE-2 system structure and knowledge processing architecture

by having an agent in an intermediate AS relay messages because the source IP address of relayed messages changes to another address and this enables the relayed messages to pass the filter.

Each agent needs a strategy that defines how to cooperate with other agents because we cannot assume that agents are located in all ASes in the actual Internet, or agents can act with a large number of agents in all diagnosis phases. For example, the strategy determines a small number of agents that an agent should first access for diagnosis. When an agent starts performing detailed analysis, the agent may need information about other topologically suitable agents. This reorganization requires an on-demand search. Such location information on the BGP topology map is maintained by an agent organization management system called ARTISTE [10], which is an independent system of ENCORE-2. ARTISTE can search agents that match a given requirement, such as "Find agents that can relay messages and are located within 2 AS-hops from ASx".

3.2 ENCORE System Structure

The ENCORE system was designed based on two assumptions: 1) An ENCORE agent can get the BGP information in the deployed AS; and 2) ENCORE does not require other, special communication facilities. ENCORE-2 consists of several modules classified according to their functions as shown in Fig. 3, and it has been modified and extended based on the design in [4]. The ENCORE-2 agent module is constructed on a network agent platform that provides basic action primitives on distributed environments. They are implemented by using Allegro Common Lisp/CLOS, although the first version of ENCORE was a hybrid system on Gnu Common Lisp, C, and Perl. ENCORE-2 agents use RPC/SSL for authentication and secure communication with each other. ARTISTE is an independent management system that organizes agents located on a BGP topology map. The knowledge processing part of an ENCORE-2 agent, which is based on the BDI (belief, desire, and intention) architecture [11], is also shown. It makes plans for verifying hypotheses, schedules executions of verification rules,

and controls monitoring and statistical analysis based on given description. In ENCORE-2, these internal modules works as threads and verification rules are also executed as threads.

3.3 Cooperative Action Management

Agent's roles in the basic cooperative strategy in ENCORE, which are *investigation*, *relay*, and *friend*, are statically assigned to perform required functions for inter-AS diagnosis. ENCORE-2 dynamically searches agents suitable for three roles based on their functional capability and topological conditions. When cooperative diagnosis is performed, an agent sends a query to ARTISTE and it then responds with a list of active agents that can perform the requested role and satisfy a given topological requirement on the BGP map. ENCORE-2 agents can also form groups where role assignments are independently defined. The formation of groups is useful from some political reasons because that can restrict possible cooperative agents and separate management information into each group.

An investigation agent is used to send back requested information observed in its environment. This role is typically assigned to agents located in major transit ASes as in ENCORE, because they can observe the large amount of routing information exchanged there. In ENCORE-2, investigation agents in transit ASes are also used at an early stage of each diagnostic action and are considered as first contact points. In the case these agents would receive a lot of queries from other agents and thus should be able to handle them. Then diagnosis starts and the next investigation agents would be designated for isolating the cause of anomalies in detail and/or identifying an area where that anomaly affects routing. An agent that resides in a stab-AS could be used as an investigation agent although the agent does not have to handle a lot of queries from other agents. A friend agent is utilized to continuously observe the state from outside the AS. In ENCORE-2, candidates for friend agents can be selected using topological requirements such as agents in a neighbor AS, a transit AS, or an AS on the other side of central ASes of the Internet. A relay agent is utilized to control the routing at the application level. If an agent cannot obtain results within a predefined time, the agent selects other investigation or relay agents and requests them to do the job. An initial set of relay agents can also be selected like candidates of friend agents.

An agent may need to find 1) other investigation agents located in ASes downstream from the initially selected investigation agent; or 2) other investigation agents located near the AS in which hijacked routes were observed. These newly selected agents are considered suitable because they could have BGP data to determine the location of the anomaly's cause or the extent to which the anomalous state, such as a hijacked route, is spreading. More comprehensively, ENCORE-2 agents are able to issue search queries to ARTISTE including condition terms such as `group`, `role`, `designated-AS`, `AS-hop-count`, and `topology`, where `topology` is `downstream`, `upstream`, or `neighbor`. Conditions can be combined using logical terms such as `and` and `or`.

4 Diagnostic Knowledge

4.1 Data Acquisition and Local Trends

According to given strategy description, ENCORE-2 statistically analyzes local data and collects analyzed results, if necessary, from multiple ASes. These include actions that are difficult for human operators: 1) Continuous cooperative confirmation of a route advertisement, which requires repeated actions of human operators over a long period. 2) Parameterization of local trends, such as the number and fluctuation of BGP full-route entries, that are also utilized as triggers for starting diagnostic actions. 3) Detailed data analysis using BGP update-level information.

Most of the trends cannot be specified as static values in advance. As an example, one agent in our AS monitors the total number of BGP route entries, which can be an important status indicator. This number differs widely among ASes and changes over time. The total number of BGP route entries in the Internet is currently over 150000 in our AS and can only be acquired through observation. According to our past records, some fatal errors in which many illegal route entries were inserted into a routing table by unintentional advertisement were detected from sudden increases in the total number of BGP entries.

In addition to providing observation functions like a human expert, an agent can provide a more detailed level of monitoring and analysis in terms of frequency and granularity for more accurate diagnostic capability. For example, an agent can monitor BGP update messages [1], while human operators usually see only a part of snapshots of the BGP routing tables in border routers. By monitoring the messages at a lower layer than what humans usually observe, the agent can recognize faults more effectively, as described in subsection 4.3. Consider the case of illegal route insertion. An agent monitoring BGP updates can detect the sudden increase in the number of update messages and easily determine that they originate from the same AS, even if unintentionally advertised routes just overwrite the legal routes and the total number of BGP entries is almost the same.

4.2 Action Strategy

Each ENCORE-2 agent has given action strategies both for the observation and diagnosis phases, which are described based on each AS's policy. For example, an agent R_{self} in AS_{self} may require a friend agent R_x to observe BGP entries and notify it of target IP addresses in AS_{self} and trap conditions. A typical trap condition is "Notify R_{self} if the origin AS number in target IP address entries is changed or some of these BGP entries disappear." When R_{self} is notified that the origin AS number is changed in AS_x, R_{self} schedules possible hypotheses for verification, which include a hypothesis that some routes are hijacked. R_{self} then gets a list of investigation agents from ARTISTE and sends queries about suspicious routes to these agents as shown in Fig. 4. R_{self} can infer the area

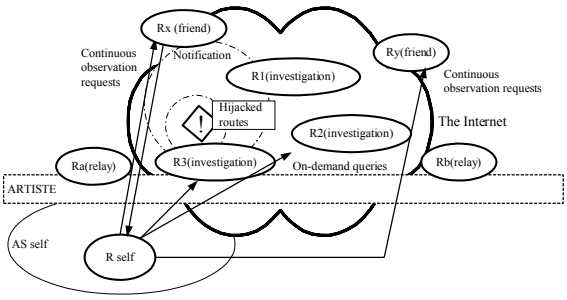

Fig. 4. Cooperative actions for analyzing hijacked route anomalies

more completely by repeatedly inquiring of investigation agents near, upstream, or downstream from ASes where unintentional advertisement is detected. The addresses of incrementally required investigation agents are also obtained from ARTISTE. In such partially hijacked cases, relay agents could effectively work to deliver messages among agents. Although serious failures like one in 1997 that disturbed all of the Internet by unintentional advertisement of full-routes might not happen because of careful filters in several major ISPs, partial or small-scale unintentional advertisement was observed several times in past few years. Thus, continuous observation in multiple ASes by friend agents and diagnosis using multiple investigation agents is yet to be useful. The former is for rapid detection and the latter is utilized to find out the area where unintentional advertisement affects reachability.

Another scenario is as follows. ENCORE-2 agent R_{self} in stub-AS AS_{self} observes various network status parameters to find indications of anomalies. In this example, suppose a border router in a transit AS, which is located upstream from AS_{self}, fails, and previous router configurations, in which a newly connected AS_{self} is not described, are restored. Then, the advertisement from AS_{self} is filtered. R_{self} finds that it cannot access some hosts, because a rule utilizing `ping` periodically fails. At the same time, friend agent R_n, which observes AS_{self} from the viewpoint of AS_n, can also find these routing changes and try to send a notify message to R_{self}. If this leads to a timeout, R_n then uses relay agents. R_{self} starts diagnosis and tries to send requests to investigation agents, which are R_x, R_y, and R_z. If direct IP forwarding from AS_x, AS_y, and AS_z to AS_{self} is impossible, this step also leads to a timeout. Then, R_{self} asks R_a and R_b to relay the previous request to AS_x, AS_y, and AS_z. Reply messages via R_a and R_b can also be delivered because R_a and R_b reside in the ASes that are not affected by the filter. According to these results, R_{self} generates the next diagnostic plans.

4.3 BGP Update-level Analysis

For a hijacked route problem, all IP addresses and their AS number in a specific AS can be registered in ENCORE-2 for verifying that the advertised routes

from the AS are not hijacked. This verification is achieved by comparing the registered information and observed results in remote ASes. In contrast, for verifying validity of routes from other ASes, the diagnostic system also has to analyze temporal sequences to accurately detect the problem, because the IRR does not necessarily reflect the current status, and the verification method using automatic comparison of the IRR data is not suited for this purpose.

The ENCORE-2 system can act as a BGP peer to monitor and record BGP update-level messages, periodically inserting a short statistical summary. This enables more detailed analysis than snapshot-based data acquisition from a routing table. In this configuration, the short summary contains the times and numbers of update messages, withdrawn routes, and advertised routes per minute. These values are used to efficiently extract the periods in which large numbers of route entries are changed. In the case of the illegal route advertising from AS_z in June 2003, we found illegal update messages from AS_z in a huge number of records. 1) We extracted update records by specifying duration using the `from` time and `to` time, which included the period when we observed some routing failures. In this example, a sufficiently large duration was used to include this period, namely 4 hours. 2) We extracted the ASes that appeared in these records more than 1000 times. At this step, there were four ASes, but AS_z appeared as the origin AS 30 times more often than the other ASes. Thus, AS_z was identified as the origin of the illegal route insertion.

4.4 Applicable Class and Limitations

From the definitions of the basic cooperative functions, this diagnostic model using a multi-agent architecture can be applied to analyze the class of anomalies whose effects can be observed as non-oscillating changes in routing information from outside an AS. According to our analysis, this class covers more than 90% of BGP-related anomalies. On the other hand, there are two types of anomaly records that cannot be analyzed in the current framework. These records belong to categories *B* and *A2*. One type was caused by oscillating changes in routing information both in the local AS and outside the AS through unintended interaction between BGP and an IGP. The second was caused by illegal interaction between the transport layer and the application layer. A hardware failure in a router prevented the router from forwarding IP packets including a specific bit sequence in the data parts. This led to repeated TCP retransmission, and these TCP sessions failed due to timeout errors. Although the latter case can be managed by adding a special heuristic rule, the number of possible hypotheses would increase significantly.

As described above, when an agent finds an anomaly of a given class and tries to diagnose it, the agent must be able to access at least one investigation agent. The model thus inherently requires access to outside the AS, meaning that it cannot cope with anomalies in which some ASes become completely isolated or inaccessible from the Internet. On the other hand, this limitation could be resolved by extending capability of relay agents to use another communication line. Note that unchanged BGP information among multiple observation points

outside the AS does not necessarily verify routing validity. There are some cases in which confirmation using only BGP information is insufficient. For example, the IP address designated by the `next_hop`, which is one of the BGP attributes, should be reachable in an AS by using some IGP. If the `next_hop` address is unreachable in the AS, IP packets cannot be forwarded there even if the BGP information is delivered beyond the AS and observed at multiple ASes. In this case, the results of `traceroute` from the outer ASes, which can be performed on the CDS, should be examined as described in a diagnostic rule to reduce the number of possible hypotheses.

5 Related Work

There are several diagnostic tools for analyzing inter-AS routing anomalies. WWW-based systems such as looking glass [9], RIS tools [12], RouteViews [13], and various visualization tools are widely used by network operators to monitor routing information and the states at specific points. These systems, however, are designed to be used by humans, and cannot be straightforwardly applied. Although analysis of temporal and topological behavior of BGP path changes [14] and centralized analysis approaches [3] were reported, all possible cases are not covered. As real-time anomaly detection by analyzing BGP updates, signature-based method and statistics-based method were proposed [15]. These methods can effectively identify anomalous BGP events, but they also cannot cover all cases. Our analysis approach about BGP update events, which utilizes a kind of learned parameters and human operator's heuristics, is less automatic than these methods, it can complementally work with them. As a hybrid system of human and statistically analyzed results [16] is unique and effective. Although it is a kind of visualization tools and cannot be directly applied, it could be complementally work if some patterns were extracted as interpretable rules. Listen and Whisper [17] can eliminate large number of problems due to misconfiguration considering network topology, but Listen only treats verification in the data plane. Whisper can verify routes in the control plane, but it requires another protocol over BGP.

Several advantages provided by the CDS-based approach would be effective to supplement them. From the viewpoints of data availability and cooperation among different administrative domains, some agent-based intra-AS diagnostic systems have been proposed, but these systems only offer restricted cooperation to obtain targeted information. These systems operate under the assumption that the targeted information exists in the management domain of the agent recognizing a problem. This means that the agents in these systems cannot deal with situations in which an anomaly or its effect is observed in a different management domain from that in which the cause exists. This situation is actually quite common in inter-AS diagnosis.

6 Conclusion

To support autonomous and stable operation in the Internet, we have proposed an inter-AS cooperative diagnostic system called ENCORE-2, which is extended through deployment in some commercial ISPs. By using ENCORE-2, an AS can continuously verify that routing is being performed as intended, and can rapidly detect and diagnose a certain class of inter-AS routing failures, which include recent major inter-AS issues such as a hijacked route problem. This CDS approach can effectively supplement other analytical methods through each agent's autonomous actions and cooperation among distributed agents considering the BGP topology.

References

1. Rekhter, Y., Li, T.: "A Border Gateway Protocol 4 (BGP-4)" (1995) RFC1771.
2. The North American Network Operators' Group: (NANOG mailing list) http://www.nanog.org.
3. Feldmann, A., Maennel, O., Mao, Z., Berger, A., Maggs, B.: "Locating Internet Routing Instability". In: Proc. of SIGCOMM, ACM (2004) 205–218
4. Akashi, O., Sugawara, T., Murakami, K., Maruyama, M., Koyanagi, K.: "Agent System for Inter-AS Routing Error Diagnosis". IEEE Internet Computing **6** (2002) 78 – 82
5. Internet Routing Registry: (http://www.irr.net/)
6. Nagahashi, K., Esaki, H., Murai, J.: "BGP Integrity Check for the Conflict Origin AS Prefix in the Inter-domain Routing". In: Symposium on Applications and the Internet, IEEE/IPJS (2003) 276–282
7. : (http://www.ntt.com/release_e/news04/0002/0226.html)
8. Mahajan, R., Wetherall, D., Anderson, T.: "Understanding BGP Misconfiguration". In: Proc. of SIGCOMM, ACM (2002) 3–16
9. Kern, E.: (http://nitrous.digex.net)
10. Terauchi, A., Akashi, O., Maruyama, M., Fukuda, K., Sugawara, T., Hirotsu, T., Kurihara, S.: "ARTISTE: An Agent Organization Management System for Multi-agent Systems". In: 8th Pacific Rim Int'l Workshop on Multi-Agents (PRIMA)(To be appeared). (2005)
11. O'Hare, G.M.P., Jennings, N.R.: "Foundations of Distributed Artificial Intelligence". Wiley-Interscience (1996)
12. RIPE: (http://www.ripe.net/)
13. Meyer, D.: (http://www.routeviews.org)
14. Chang, D., Govindan, R., Heidemann, J.: "The Temporal and Topological Characteristics of BGP Path Changes". In: Proc. of Int'l Conf. on Network Protocols, IEEE (2003) 190–199
15. Zhang, K., Yen, A., Zhao, X., Massey, D., Wu, S., Zhnag, L.: "On Detection of Anomalous Routing Dynamics in BGP". In: Proc. of Networking, IFIP (2004) 259–270
16. Teoh, S., Ma, K., Wu, S., Massey, D., Zhao, X., D.Pei, Wang, L., Zhang, L., Bush, R.: "Visual-Based Anomaly Detection for BGP Origin AS Change (OASC) Events". In: Proc. of 14th IFIP/IEEE DSOM. (2003) 155–168 LNCS2867.
17. Subramanian, L., Roth, V., Stoica, I., Shenker, S., Katz, R.: "Listen and Whisper: Security Mechanisms for BGP". In: Proc. of Networked Systems Design and Implementation, USENIX (2004) 127–140