

Responsive Event-Driven Safe and Secure Information Sharing Platform

Hiroshi Ishii Department of Information, Telecommunication and Electronics, School of Information Science and Engineering, Tokai University Hiratsuka, Kanagawa, JAPAN	Chee Onn Chow Course of Science and Technology Graduate School of Science and Technology Tokai University Unified Graduate School Hiratsuka, Kanagawa, JAPAN	Masahiro Yamamoto Course of Computer and Communication, Graduate School of Engineering, Tokai University Hiratsuka, Kanagawa, JAPAN	Sakurako Horie ADOC International Co., Ltd. Tachikawa, Tokyo JAPAN	Hiroaki Nishikawa Department of Computer Science, Graduate School of Systems and Information Engineering, University of Tsukuba Tsukuba, Ibaraki, JAPAN
---	---	--	---	--

Abstract

Recently, disasters are often striking the earth. In case of those emergency cases, information sharing infrastructure is highly required to be available with minimum security. This paper proposes a basic concept of responsive event-driven safe and secure information sharing platform to respond the above requirement. Our idea is twofold. One is the robust ad hoc network concept. When hosts and terminals may lose accessibility to the existing infrastructure after the emergency, we propose to establish wireless ad hoc network environment with information-oriented routing and route multiplication for safety. The other is the data-driven platform to support the safe and secure information sharing, which achieves efficient real-time multi-processing capability without any runtime overhead based on the passive or data-driven execution mode. By virtue of the processor, we apply it to continuous packet filtering for security and multiple job handling.

Key words: Internet worm, security, ICMP, intrusion detection

1. Introduction

It becomes realistic to have a ubiquitous networking society which people can take advantage of information sharing environment anytime and anywhere [1]. The studies so far, however, mainly tackled so-called “usual situation”. Recently, disasters often strike in a global size because of abnormal climate and human activities [2]. If natural disasters and in some cases terrorism attack metropolitan areas where infrastructures are well installed, the damage infrastructures must suffer will be terrible.

Hence, it is urgently required to establish the information sharing environment that can be securely used in case of emergency. At the same time, it is doubtless minimum assurance of security of communication will be required even in emergency.

To achieve above emergency information sharing environment, comprehensive study must be necessary from the hardware platform through the network layer to application.

First, the hardware platform [3][4] that will support the information sharing platform will have to be tolerant to multiprocessing and congestion of processes in unstable condition of emergency case, and consume as little electric power as possible. And it will be efficient if pattern check for viruses and worms is realized in the hardware layer.

In the network layer, it is likely to happen for hosts and terminals to lose accessibility to existing infrastructure in case of emergency. In this case, it seems the wireless ad hoc network [5] can be a useful communication environment, which can set up a local network connecting to neighboring hosts. In emergency case, it is highly required to find such important information as where water, food, shelter, medicine, and hospitals are. Hence, information discovery mechanism is a very indispensable issue in emergency ad hoc network. Moreover, considering unstable network condition, it will be needed to have diversity in route and information transmitter.

In upper layer, it will be required to have some authentication mechanism without usual security infrastructure because even in emergency minimum security will be assured.

This paper proposes a concept of responsive event-driven safe and secure information sharing platform to achieve above objectives by synthesizing application, network and hardware platform.

Section 2 discusses the requirements to the information sharing platform in emergency such as natural disasters. Section 3 proposes emergency ad hoc network architecture. Section 4 describes data-driven processor platform to achieve the requirements. Section 5 summarizes the discussion.

2. Requirements for Safe and Secure Information Sharing Platform

Ubiquitous communication provides information communication environment anytime and anywhere [1]. The keyword, anytime, is always true? Recently heavy natural disasters often attack such as storm, flood, tsunami, and landslip. In such a case, to keep or urgently restore infrastructure is indispensable. The information sharing infrastructure including information and communication services and its facilities is one of the most important infrastructures. The requirements to make information sharing platform to be available “anytime” would be as follows.

2.1 Requirements for the hardware platform

In case of emergency, hardware platform [3][4] must be tolerant to heavy load and simultaneous multiple processing such as many node discovery message handling and frequent routing information control to establish mobile ad hoc network as described in 2.2.

Since ad hoc networks always exchange and process network configuration information such as routing messages, it is not desirable for normal processing to be loaded by the network configuration processing.

More over in some case, it may be very effective to continuously execute the pattern file checking for internet virus and worms in the hardware layer in order to keep security and safeness in the overall ad hoc network.

Hence, real-time multi-processing capability without any runtime overheads is required for the hardware platform.

Also in emergency, power feeding also becomes a problem. The hardware must reduce as much as power consumption as possible.

2.2 Requirements for the network layer and above

It is highly possible for hosts and terminals to lose accessibility to the communication infrastructure whichever wired or wireless is in case of such emergency as disasters. To make a quick recover of the communication capability in this situation, wireless ad hoc network could be a good alternative to the lost infrastructure.

Mobile Ad hoc networks [5] are defined as a group of wireless devices that are capable of organizing themselves in a mesh topology in order to find routes and relay packets from a node to any node within the network without the support of any fixed infrastructure.

The routing in the ad hoc network is made assuming every node knows addresses and/or names of the

communication opponents. But in the initial stage of the emergency ad hoc network establishment, it is likely that nodes do not know who are in the same ad hoc network. So, some means to discover the opponents will be needed.

Especially in the case of emergency, there is a case where specific address is not necessary but specific information owned by the nodes is. For example, people would like to know where medical doctors are, where drinking water is, and so on. They need no specific IP address. This is “information or contents discovery mechanism which must be required in the emergency network.

This type of discovery mechanism is generally adopted in the P2P environment using the existing infrastructure but not well discussed for the ad hoc network.

And after information discovery, layer 3 routing must be executed. In the ad hoc network, the routes are not stable due to mobility and some more wireless specific conditions. So, to assure the information transfer, some efficient diversity mechanism will be needed.

In upper layer than layer 3, minimum security will be required. If the PKI (Public Key Infrastructure) [6][7] does not work well in the emergency, some alternative mechanism of authentication, ciphering, and virus checking mechanism will be needed.

3. Emergency network formed by wireless ad hoc network (Robust ad hoc network)

3.1 Information discovery mechanism

As discussed in section 2, in case of emergency, it is highly required to discover necessary information as soon as possible. The IP addresses and server name are not actually useful in the initial phase of emergency because the DNS might not work well and geographical distance is not clear to know whether the host with the destination address is in the same ad hoc network as the source node belongs to. Hence, some mechanism to discover the communication opponent is needed.

Let us consider what the keys for discovery are. First, the specific information owned by each node is the most possible key. For instance, people want to know where medical doctors are, where drinking water is, and so on. Second, the specific group is also a good key for discovery. You would like to discover your community such as your company, school, and so on. Third, specific names and addresses could be used.

We propose a mechanism of discovery for two directions. One is “push” typed, the other is “pull” typed.

(1) PUSH mechanism

As for the push typed discovery, we have already proposed “Words-of mouth information sharing mechanism based on MPR” [8]. Information owner broadcasts a PUSH packet informing the fact that he has the information or catering information itself by using flooding mechanism. To reduce total broadcast packets, we adopt MPR (Multi-Point Relaying) [9]. If a node that needs the information in the PUSH packet receives the packet, he can discover the source. Then, layer 3 routing information must be discovered.

(2) PULL mechanism [8]

We also added inquiry mechanism in the above mechanism, which will be categorized into Pull mechanism. When people would like to know a place where specific information is, he sends a PULL packet for inquiry. If nodes hearing this PULL packet have cache of a PUSH packet which contains same information as the PULL does, they will at once send back the PUSH packet to the PULL sending node. Then, layer 3 routing will be begun.

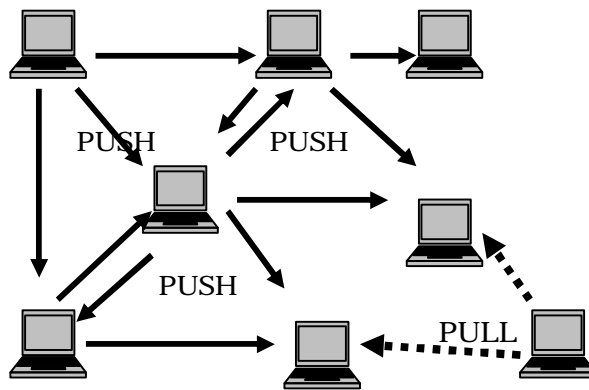


Fig. 1 PUSH and PULL

3.2 Route discovery

A node who wants the information notified by a PUSH packet, it will start route discovery mechanism in layer 3. To enable effective route discovery, the path information, a sequence of addresses the PUSH packets passed through, is assumed to be recorded in PUSH packet.

Considering the less stability of the emergency ad hoc network, it might be better to have diversity in routes. Diversity can be considered in several senses. One is the case where a source has multiple routes to diversify the same traffic. The other is source diversity. This is the case where you can find the same data in different nodes mirrored, which is a kind of source diversity. Depending on the route information got by the PUSH packet, a node will select appropriate route diversity.

Especially for the video transmission over the mobile ad hoc network, we have proposed a multipoint-to-point video transmission mechanism [10], by modifying existing routing mechanism, DSR (Dynamic Source Routing) [11].

3.3 Security mechanism

Even in emergency, minimum security might be required. It is likely for the PKI not to work well in the emergency and some alternative mechanism of authentication, ciphering, and virus checking mechanism will be needed.

Let us consider the case where a node would like to talk to a server node over ad hoc network. Now, those two nodes know mutually the names and/or addresses but they cannot rely on each other.

There are several ideas to enable the secure communication in this case.

First, before the emergency, the server has been certified by a CA of PKI and the server has a certified public key in a limited duration of time. If a non-server node which does not have any certified public key is certified by the server in some means, the node can be an authorized node in the ad hoc network and can use its own public key. The more the authenticated nodes increase, the more securely communication over the ad hoc network can be made.

The other idea is "Guild" system. Considering possible emergency, each node belongs to a community such as a company, school and so on beforehand. It has an emblem containing a list of message digest of MAC address of guild member nodes. After the emergency, each node exchanges its emblem and knows the opponent is a member of the guild.

As for the virus attack, we are considering to embed the function onto the data-driven processor as described in section 4.

4. Multi-Media Networking-Oriented Data-Driven Processor: CUE

To realize a secure networking infrastructure, the authors are carrying out CUE (Coordinating Users' requirements and Engineering constraints) project. This research currently aims at building ubiquitous networking-oriented data-driven real-time execution platform.

In the CUE project, the authors first realized emulation facility having prototyping functions of dataflow late and turnaround time named RESCUE (Real-time Execution System for CUE series data-driven processors)[12].

In the first stage of the research, effectiveness of these functions was proven through protocol handling program developments by RESCUE. That is, CUE project was inaugurated in 1995 by feasibility study on possible data-driven implementation of real-time multiprocessing essentially needed in protocol handling for multi-media networking environment.

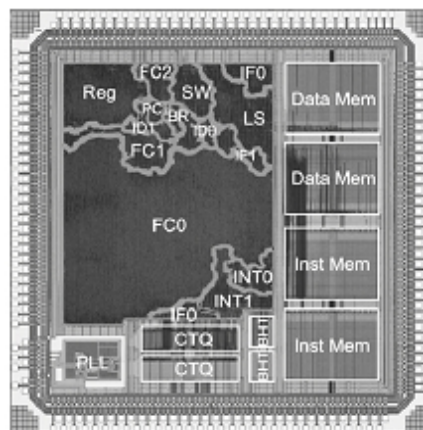
In order to keep maximum throughput in our data-driven processor, the basic design target for real-time multiprocessing scheme was chosen so as to alleviate any runtime overheads and to achieve real-timeness in the protocol handling without any supervisory controls.

Finally, data-driven parallel realization of protocol handling demonstrated efficient real-time multi-processing capability without any runtime supervisory control as long as data length is appropriate as shown in [13].

The RESCUE also showed that sequential parts of real-time programs frequently encountered in actual time-sensitive applications such as connection/port management in TCP and the serialization of parameters in video compression result in bottlenecks in data-driven execution. Since data-driven architectures cannot exploit the locality of computation, it is not good at sequential processing. This is the compensation of exploiting fine-grained parallelism.

To alleviate this issue with retaining the advantages of pure data-driven architecture, architecture of the latest version named CUE-v2 [14][15] was established as a hybrid processor enabling simultaneous processing of data-driven and control-driven threads to achieve higher performance for inline processing and to avoid any bottlenecks.

The prototype chip was developed by employing standard-cell design, and it was implemented using timing-driven synthesis/layout. Crosstalk, antenna effect, and voltage drop were analyzed and validated using commercial EDA tools. The chip is built in a generic 0.18um six-metal layer process, the die size of 5 x 5 mm², including 64 kbyte SRAM, and is packaged in a ball grid array having 292 pins. The chip layout is shown in Fig.2.



IF0,1: Instruction Fetch 0,1 ID0,1: Instruction Decode 0,1
FC0,1,2: Firing Control 0,1,2 INT0,1: Integer 0,1 LS: Load/Store
BR: Branch Reg: Register file CTQ: Control Thread Queue

Fig. 2 Layout image of the CUEv2

The chip was verified with several applications. It proved to work without any significant flaws in this chip. Most of its functional verification time was spent for an out-of-order scheduling of control-flow. The verification for basic operations and the simultaneous processing of dataflow and control-flow threads was not dominant. Thus, the CUE-v2 architecture is not more complex than superscalar processors. The CUE-v2 chip will be installed to PCI board in Fig.3, which was originally designed in the CUE project, to be examined for its potential capability as chip multi-processor core in the next generation CUE-v3, which will achieve around 40 Giga bit per second through wireless network interface.

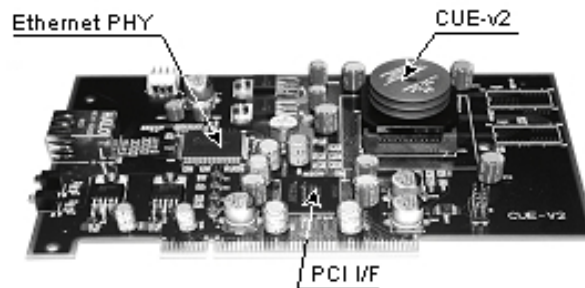


Fig.3 CUE-v2 PCI board

In CUE project, elastic pipeline realization has been experimentally verified for turn-around time and throughput in a circular pipeline adopted as a chip multi-processor core in the CUE-series data-driven multi-processors. Through VLSI realizations of CUE-p and CUE-v1, the turn-around time keeps minimum value as far as over loaded condition is avoided. This nature of the pipeline fully utilized in the real-time multiprocessing discussed in Section 2.1. Also, it was experimentally verified that power consumption of our data-driven processors was in proportion to throughput achieved in the pipeline. This feature and passive operation mode in ready-to-fire principle of the data-driven scheme will be effective to minimize power consumption at standby time.

Fully utilizing throughput, multi-processing capability and real-time responsibility CUE-v3 will be one of the most promising platform to realize the robust ad hoc network in our project.

5. Summary

This paper discusses and proposes a concept of Responsive Event-Driven Safe and Secure Information Sharing Platform encompassing layers from application to hardware platform.

One of the main ideas is the robust ad hoc network concept. When hosts and terminals may lose accessibility to the existing infrastructure after the emergency, we propose to establish wireless ad hoc network environment with node discovery mechanism by using information owned by them. After getting the location of information, route discovery and route multiplication mechanisms are proposed for safety. On top of the robust ad hoc network, we propose a way of authentication by use of ex-PKI and MAC address based guild system.

The other is the data-driven platform to support the safe and secure information sharing, which achieves efficient real-time multi-processing capability without any runtime overhead based on the passive or data-driven execution mode. By virtue of the processor, we apply it to continuous packet filtering for security and multiple job handling.

By combining these ideas above, we believe we can establish a new paradigm for emergency information sharing. We are going to implement proposed systems to show the effectiveness of the proposal.

Acknowledgment

The research is partially supported by SCOPE (Strategic Information and Communications R&D Promotion Programme), Ministry of Internal Affairs and Communications, Japan.

Chow would like to thank the Hitachi Scholarship Foundation for its support.

References

- [1] Ministry of Public Management, Home Affairs, Posts and Telecommunications, Japan, "White Paper Information and Communications in Japan" <http://www.johotsusintokei.soumu.go.jp/whitepaper/>
- [2] United Nations, "Living With Risk: A Global Review Of Disaster Reduction Initiatives", United Nations Pubns, ISBN: 9211010500, 2004
- [3] J.R.Allen, Jr., et al., "IBM PowerNP network processor: "Hardware, software, and applications, "IBM J. DEV. Vol.47 No.2/3 March/May (2003).
- [4] Muthaiah Venkatachalam, "Integrated Data and Control Plane Processing Using Intel** IXP23XX Network Processors," Intel(R) Feb. (2005).
- [5] B. Xu, S. Hischke and B Walke, "The Role of Ad Hoc Networking in Future Wireless Communications", Proc. Intl. Conf. on Communication Technology, ICCT 2003, Beijing, China, vol. 2, pp. 1353 – 1358, April 2003.
- [6] ITU-T Recommendation X.509
- [7] IETF Public-Key Infrastructure (X.509) Working Group (pkix) <http://www.ietf.org/html.charters/pkix-charter.html>
- [8] M. Yamamoto and H. Ishii, "A Study on Word-of-Mouth Information Sharing based on MPR", IEICE Communication Society Conference 2005, B-21-49 (in Japanese), Sep. 2005
- [9] A.Qayyum, L.Viennot, and A.Laouiti, "Multipoint relaying: An efficient Technique for flooding in mobile wireless networks", Technical Report 3898, INRIA-Rapport de recherche, March 2000
- [10] C.O. Chow and H. Ishii, "Interactive Video Transmission over Wireless Ad Hoc Networks using Multiple Sources and Multiple Description Coding," 6th Asia-Pacific Symposium on Information and Telecommunication Technologies (APSITT2005), pp.305-309, Yangon, Myanmar, Nov. 2005
- [11] D. B. Johnson, D. A. Maltz, Y. C. Hu and J. G. Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks", IETF Internet Draft, draft-ietf-manet-dsr-10.txt, July 2004.
- [12] Yasuhiro Wabiko and Hiroaki Nishikawa, "Performance Prediction and Verification Environment for Super-Integrated Data-Driven Processors; RESCUE," Transactions of the Society for Design and Process Science: Journal of Integrated Design and Process Science, Vol.5, No.4 Dec. 2001
- [13] H. Ishii, H. Nishikawa and Y. Inoue, "Data-Driven Implementation of Highly Efficient TCP/IP Handler to Access the TINA Network," IEICE Transactions on Communications, Vol. E83-B, No. 6, pp. 1355-1362 Jun. 2000
- [14] S. Ito, R. Kurebayashi, H. Tomiyasu, and H. Nishikawa, "A Processor Architecture for Simultaneously Processing Dataflow and Control-flow Threads," Proceedings of the 15th IASTED International Conference on Parallel and Distributed Computing and Systems, pp.339-344 Nov. 2003
- [15] H. Nishikawa, "Design Philosophy of a Networking-Oriented Data-Driven Processor: CUE", IEICE Transaction on Electronics, VOL.E89-C NO.3, pp.221-229 Mar. 2006