2005－ＭＢＬ－33（15）
2005／5／26

MobiSNMP：SNMP over Mobile IPv6による移動体情報の継続的収集手法

北形 元[†] 小出 和秀[†] 神山 広樹[†] GlennMansfield Keeni[††] 白鳥 則郎[†]

† 東北大学電気通信研究所/情報科学研究科
〒 980-8577 仙台市青葉区片平 2-1-1
†† (株) サイバー・ソリューションズ
〒 989-3204 宮城県仙台市青葉区南吉成 6-6-3 ICR ビル 3F
E-mail: †{minatsu,koide,kamiyama,norio}@shiratori.riec.tohoku.ac.jp, ††glenn@cysols.com

あらまし 本稿では，実環境における既存のネットワーク情報収集手法の信頼性の欠如に関する解析を行い，SNMPを用いたワイヤレスモバイルエンティティのための新しいネットワーク管理手法：MobiSNMP を提案する．本提案のキーアイデアは，ストア＆フォワード型の管理オブジェクト (MO:Managed Object) を導入することにある．提案手法により，マネージャとエージェント間の接続が失われている間にも，エージェントが収集すべき情報をキャッシングし，情報の欠落を防ぐ．本稿では提案手法のプロトタイプ実装を行い，プロトタイプを用いた実験を通じ，提案手法の有効性を示す．

キーワード 情報収集, MobileIP, SNMP, ストア＆フォワード機構, 実環境

MobiSNMP - Continuous Information Collection from Moving Entities using SNMP over Movile IPv6

Gen KITAGATA[†], Kazuhide KOIDE[†], Hiroki KAMIYAMA[†], Glenn MANSFIELD KEENI[††], and Norio SHIRATORI[†]

† Research Institute of Electrical Communication/Graduate School of Information Sciences, Tohoku University
2-1-1 Katahira Aoba-ku,Sendai, 980-8577, JAPAN.
†† Cyber Solutions Inc.
ICR bld 3F 6-6-3 MinamiYoshinari Aoba-ku Sendai-shi, 989-3204, JAPAN
E-mail: †{minatsu,koide,kamiyama,norio}@shiratori.riec.tohoku.ac.jp, ††glenn@cysols.com

Abstract In this paper, we analyze the unreliability of existing information collection methods in the real-world MobileIP environment. We focus on this problem and propose a novel network management model MobiSNMP that anticipates the wireless mobile entities and uses SNMP. The key idea of this model is the introduction of a *store-and-forward* type Managed Object (MO). During the period of unreachability between the Manager and the agent, the data is cached at the agent until the connectivity recovers. In our experiment we used a prototype implementation in real-world wireless communication field, and showed the effectiveness of our proposed method.

Key words Information collection, MobileIP, SNMP, Store-and-Forward mechanism, Real-world environment

1. Introduction

The continuous growth of the Internet and the rapid development of mobile communication devices from lightweight laptops to PDAs has made host mobility necesssary over the Internet. The needs of mobile ubiquitous network connection is growing. Wireless connectivity services have been realized.

MobileIP is the current standard protocol for supporting *mobility* in IP networks. In IPv6 mobility is an embedded feature. MobileIPv6 [1] protocol is already standardized and it is likely to be deployed in a large scale. Research and development of management and monitoring system for MobileIP network is on-going. The management information base module for MobileIPv6, MobileIPv6-MIB [2] is under discussion for standardization. This is the Management Information Base to manage MobileIPv6 entities using SNMP [3]. Other than management information we can collect useful information of a host by SNMP from the mobile entity.

Though considerable work has been done on MobileIP, the discussion on the method of effective information collection from mobile entities is still inadequate. The basic assumption in existing management systems is that the managed node is always connected and reachable. But in wireless mobile environment, reachability of nodes is quite unreliable.

In this paper, we first analyze the unreliability of existing information collection methods in real-world MobileIP environment. Then we propose a novel network management model MobiSNMP that anticipates wireless mobile entities and uses SNMP. The key idea of this model is a *store-and-forward* type Managed Object (MO). This MO maintains cached information about other specified MO and serves as a backup repertoire, in case the connectivity between the agent and the data collector has recovered after a disruption.

The remainder of the paper is organized as follows. A more detailed description of the problem of data collection from mobile entities is given in Section 2. In Section 3, we propose a new model for robust information collection in an unreliable communication environment. Implementation issues are discussed in Section 4, and in Section 5 we present the experimental results. Conclusions and future works are in Section 6.

2. The problems of data collection from mobile entities

2. 1 The present data collection model

The existing standard remote management and monitoring model is the *agent-manager* model adapted in SNMP network management framework. This is essentially manager-led information collection. In this model, agents provide information passively. Manager decides what information will be collected and how this information will be collected.

This model is simple and flexible but unreliable. The merit of this model is, it enables various managers to access the same agents with their respective information collection strategy. The activity of agents and managers are independent. But the drawback of this model is if the agents, or connectivity to the agents, go down for some reason, the information collection by managers will fail and there is no way to recover the lost data.

2. 2 The problems of data collection in a mobile environment

The model mentioned above assumes that agents and managers are in a static condition, and are connected to wired-network. Actually, in wired networks, the *unreliability* of this model is not a big issue. However, this is not the case in wireless networks. Wireless networks are prone to noise, disturbance, and intermittent discontinuities. Those adverse conditions affect network reachability and consequently data collection.

We have experimented in a real-world situation [4]. The experiment focused on evaluating MobileIP for transferring vital information of a patient from an ambulance approaching the hospital, in realtime and continuously using wireless connections. The experiment setup is as shown in Fig. 1

Fig. 2 shows the pattern of traffic in this experiment while transferring vital information of a patient in realtime. Mobile Node (MN) is inside the ambulance and the hospital monitors the information using a Correspondent Node (CN). All traffic passes through the Home Agent (HA). MN uses two kinds of wireless link, (i) Digital Wireless Link (DWL) and (ii) EV-DO. IP-IP tunnel line shows the DWL's s traffic, and 9999/TCP shows the traffic pattern between HA and CN. In this graph, the handover occurred when DWL's traffic is cut off. Due to handover latency there is a gap in EV-DO's traffic. A major problem in this case is that the data collection from Mobile Node will stop using any information collection method. A second problem is a nature of the traffic when the connection is reestablished. A very large spike appears in (ii) due to the buffering of packets. In general, the bandwidth of wireless links is relatively narrow and such kind of burst traffic will adversely affect the data collection activity.

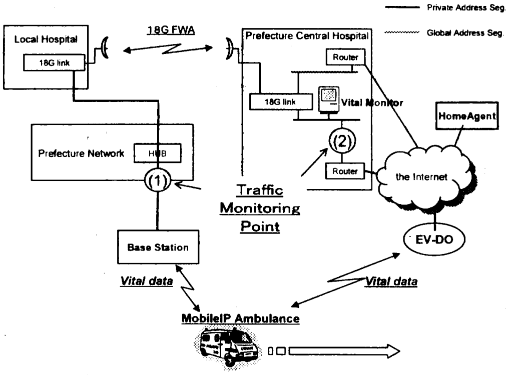

Figure 1 Experiment on vital information transfer(Dec./04/2004, Miyagi Prefecture, JAPAN).

When handover occurs, the flow of vital information is

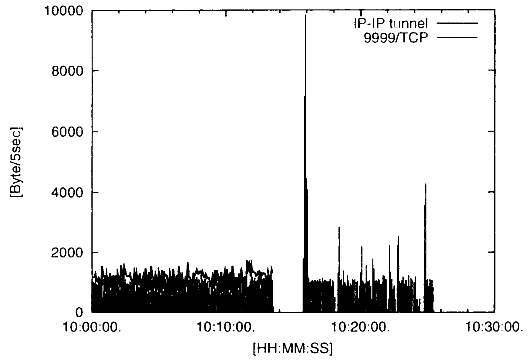

Figure 2 Problem in MobileIP(Experiment in AM10:00-11:00, Dec./04/2004, Miyagi Prefecture, JAPAN).

disrupted. This is a major problem as the vital information needs to be accurate and continuous for useful medical analysis.

In such an environment, the unreliability of the existing monitoring model cannot be ignored. We envisage *reliability* for remote information collection as follows:

(1) Agents indicate the loss of connectivity to the managers.

(2) Agents recognize the information, managers will collect (such as, *type of information*, *time interval*, etc.)

(3) Agents cache the information until connectivity recovers.

2.3 The solutions

The reasons of discontinuities can be classified as follows :

- predictable discontinuities
- unpredictable discontinuities

Long-term, predictable discontinuities will occur due to network failure. Short-term, predictable discontinuities will occur, for example in handover of Wireless LAN or Mobile IP. In those cases, *trap-oriented* solution will be better. In the *trap-oriented* solution agents look for indications of a disconnection and send *traps* until reachability to managers is lost. The agents will (re)start sending *traps* when reachability has recovered. Managers will stop polling until connectivity recovers.

On the other hand, disconnection by media noise or suspension of agent are unpredictable cases. In this case, polling based solution will be better. Agents should always cache information in its local buffer, and managers should poll and fetch the result as a block-data when the agent is reachable. This can be called the *cache-solution*.

The load of the agents will be less in the former approach, but the mechanism is complicated. Also, this strategy does not suit the unpredictable situations well. Though the latter case suits the predictable case well, the cache maintenance activity will cause the load of agents to be higher.

In this paper, we adapt the latter strategy and propose a reliable information collection model.

2.4 Evaluation of the pros and cons of the various solutions

Application and system oriented remote monitoring approaches are found in telemedicine area [5]~[8]. These systems are useful for some situations such as monitoring the condition of a patient's vital data in a hospital or monitoring electrocardiograms from moving ambulance. However, they assume homogeneous network, e.g., wireless local area network (WLAN) such as IEEE 802.11 or wireless wide area network (WWAN) such as cellular network. Therefore they can be used for in-house or outdoor purposes exclusively.

On the other hand, many kinds of efficient handover methods for heterogeneous wireless networks are proposed from the view point of wireless link layer [9]~[11]. These methods compare signal strengths of different radio access networks such as WLAN and WWAN, then switch WLAN and WWAN. By applying those methods to remote monitoring system mentioned above, we can monitor mobile nodes from in-house to outdoor seamlessly. However, discontinuities still exist due to several reasons such as shielding of radio wave by buildings or signaling latency of Mobile IP protocol [1].

To cope with the discontinuities of network and avoid loss of part of continuous monitoring data, there is an urgent need of a robust information collection method which recovers missing data lost by the discontinuities.

3. MobiSNMP: A model for robust information collection in an unreliable communication environment

3.1 MobiSNMP: The model

We propose an agent-oriented information collection model. The characteristics of this model is that an agent contains *Information Interface*(I-I/F) and it works as the proxy of the managers. The Interface of an agent collects and stores data continuously in a cache with timestamps. Manager can fetch this information in a block when the agent is reachable, because the data contains time-stamp information. Here we adapt a *store-and-forward* information collection strategy. Agent's clock should be synchronized with ntp or GPS clock.

Of course, the I-I/F needs to know the kind of information accessed by managers. An I-I/F should keep a configuration of managers. It is possible that **Manager-A** collects data in 1 minute intervals, and **Manager-B** collect the same data at 5 seconds intervals. If I-I/F stores the data in 1 minute intervals in the cache, it will not be able to cater to **Manager-B** requirements. In this case the I-I/F should keep data at

5 second intervals, i.e. the greatest common divisor of the manager's polling interval time.

The overview of the proposed model described above is shown in Fig. 3.

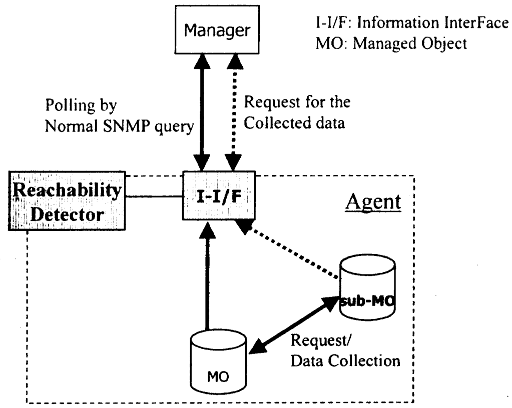

Figure 3 Proposed Model: Agent-leading information collection with Information Interface and sub-MO.

3.2 Analysis of the degree of robustness

There are two important points in our methodology of *reliability* in information collection:

(1) Time taken for recovery

(2) The amount of lost data

Point 1 is important in our work as we focus on *online information collection.* As discussed in Section 2, there are applications where information needs to be processed in realtime.

Point 2 is another metric. In a real-world environment, there will always be a non-zero probability of partial lose of data. In cases where the bandwidth of the wireless link is narrow, and transferred data could not reach the manager, the proposed model provides a way to fetch the lost data quickly using an aggregation mechanism, explained in the next section.

4. Implementation

We implemented the proposed MobiSNMP within the SNMP framework. As base we used the *net-snmp* package, the popular free SNMP agent program available. We define a special MIB named *idtpMIB* to represent the cache of stored information. *idtpMIB* is structured as a back-end module and a front-end module. The back-end module accesses the configured MO locally and caches the information along with the time-stamp. This realizes I-I/F feature of the agent. The front-end module serves the cached information to the SNMP requesters.

We have to define the interval at which the back-end *idtpMIB* polls and stores the information. The data collector should detect the failure of polling, and attempt recovery by trying to access the backup cache in the agent via the *idtp-MIB* module. It is up to the data collector to maintain the proper sequence of the data by comparing the timestamps of the collected data.

Fig. 4 shows the diagram of the prototype system we implemented.

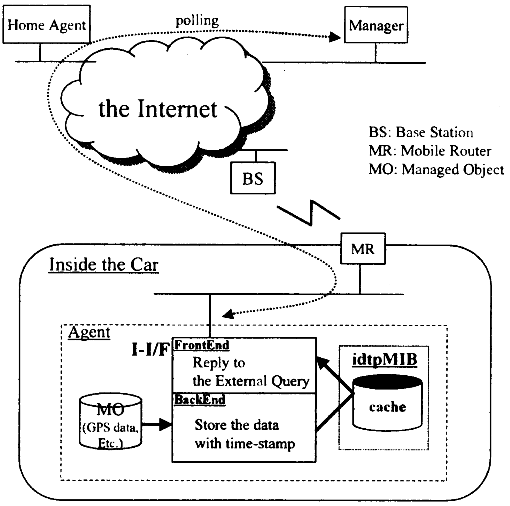

Figure 4 Implementation of proposed system.

5. Experiment and results

There are two metrics that need to be evaluated:

(1) Time taken for recovery

(2) The amount of lost data

In evaluating the first metric, we deploy the prototype implementation of proposed method on the static wired host. We simulate link cut-off and measure the recovery time of data.

We evaluate the second metric, using real-world wireless communication environment. We deploy the developed system on the MobileIPv6-ready SNMP probe on a car. Normal polling data from the probe is collected for nearly 1 month (Dec./04/2004-Feb./12/2005) as a base data, and examine the effectiveness of our proposed method for a single day experiment.

5.1 Time taken for data recovery

In our experiment the Manager makes a continuous polling to the agent at 10 seconds intervals, and we periodically disconnect the agent interface. We set the time of disconnection at 30 seconds, 60 seconds, 300 seconds and 600 seconds . So naturally Manager will fail to collect data during these disconnected phases. For example, when the disconnection time duration is 300 seconds, the Manager will loss polling for 30 times. We initiate these disconnection sequentially with 3 minutes intervals, and repeat them for 10 times.

While connected, the Manager accesses the *idtpMIB* module of the agent at 60 seconds intervals. After the disconnection phase, when it regains the connection, the manager accesses the *idtpMIB* module more frequently. In this case, in every second, for a quick recovery of the lost data. In this way Manager can recover 6 data block per second of *idtpMIB* polling. One such case is shown in Fig. 5. To give a clear view of fast recovery, we have expanded this figure in Fig. 6, which shows the gradual reducion of delay from 840 seconds to 240 seconds. Here Manager polls *idtpMIB* in every second for 10 times and recovers 300 lost data.

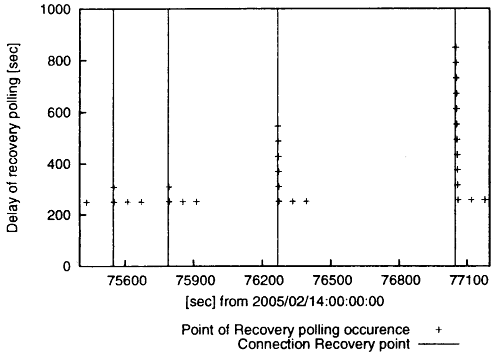

Figure 5 Delay of data recovery: Recovery after 30sec, 60sec, 300sec, 600sec disconnection.

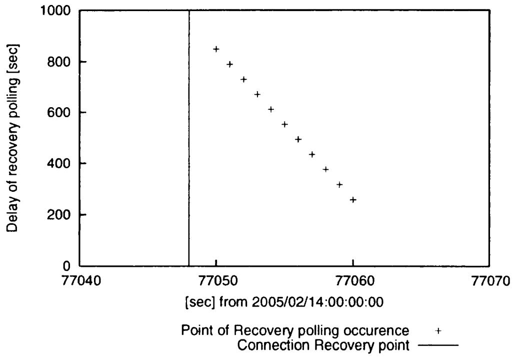

Figure 6 Delay of data recovery: fast recovery in 1 second interval.

In both Fig. 5 and Fig. 6 the y-axis represents the delay time of recovery polling. Those figure shows that the minimum delay time for recovery polling is nearly 240 secs. This comes from the implementation of *idtpMIB* module. The delay of first recovery polling should be (600 $seconds = 5minutes) + default$ 240 $seconds\ delay$ = 840 $seconds$ as shown in Fig. 6. Recover pollings are carried out more frequently than normal pollings, and the delay decreases as the recovery process progresses.

Time required to recover the lost data is shown in Table. 1. These data confirms the speedy recovery. This fast recovery process considerably improves the stability of realtime continuous monitoring.

Table 1 Data recovery time after re-connection.

disconnection length (sec)	recovery start delay (sec)		recovery duration (sec)	
	Mean	SD	Mean	SD
30	2.60	1.91	0.51	0.51
60	2.21	1.17	1.00	0.01
300	2.00	1.68	5.10	0.30
600	1.89	1.60	10.12	0.32

5. 2 The amount of lost data

In this section we evaluate the amount of lost data, and recovered data in the real mobile environment.

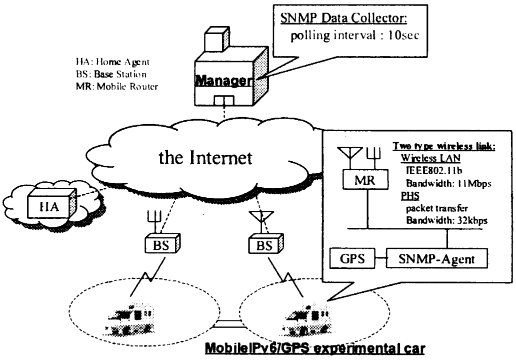

Figure 7 Experimental Environment: monitoring MobileIPv6 car with WLAN and PHS.

Fig. 7 shows the experimental environment. There is an on-board wireless MobileIP router and the on-board probe computer. This computer collects information from various probes and serves it to the data collectors via SNMP. The router and the probe computer are connected to the car's LAN. The router has two types of wireless interfaces. One of them is IEEE 802.11b wireless LAN interface with the bandwidth of 11 Mbps, and the other is a PHS packet transfer interface with a bandwidth of 32 kbps.

We deploy the snmp agent with our proposed *idtpMIB* and GPS on the probe computer. When the car moves, the location information will be updated and can be remotely monitored using SNMP.

Here we adapt *GPS-MIB monitoring* as the test case of data collection in this experiments. We consider this monitoring as a realistic application that will be used to track the car's movement. The application needs *realtime* and *continuous collection* of information.

In this experiment, we set the $timeout = 30minutes$ to the polling management. If the polling failure persists for 30 minutes, the manager will decide that the car is in ignition-off state. We don't consider such situation as *data-collection-failure*.

We collected normal polling data from the probe computer on the car for nearly 1 month (Dec./04/2004-Feb./12/2005). Fig. 8 shows the number of *polling-trials*, *successful polling-count*, and the *rate of failure* of polling per day. This result shows that in normal cases a considerable amount of data is lost.

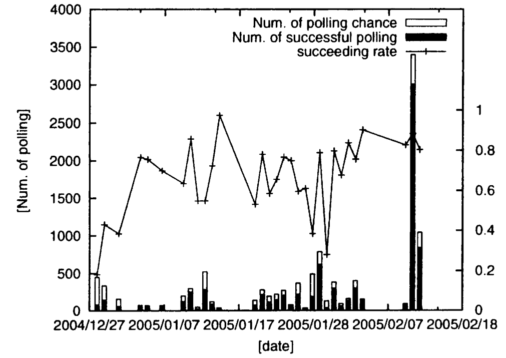

Figure 8 Polling failure rate per day (Dec./04/2004-Feb./12/2005 Experiments).

On the other hand Fig. 9 shows the loss rate of polling with proposed method. We make an experiment of polling with normal polling and recovery method using *idtpMIB-system* in parallel. This shows the result for 2 hours (Feb./12/2005 17:00:00-19:00:00). Our system succeeded to recover almost half of failure cases' data. The first part of Fig. 9 (0-17:30:00) shows heavy loss of polling data. Here we stopped the engine of the car and shut down the mobile server after we verified the bootstrapping of the mobile server. As the engine was stopped, so naturally there is no data available during this period of time. But in the latter part of Fig. 9 (17:30:00 onwards) shows our method's remarkable robustness in recovering lost data, when the car passes through the tunnel, i.e. for a certain period of time without connectivity. This results clearly shows that our proposed model achieved sufficient improvement in reducing polling loss rate in the actual real-world situation.

6. Summary and Conclusion

In view of the inadequacies of existing remote information collection models and their lack of reliability in wireless mobile communication environment, we proposed MobiSNMP which has a *store-and-forward* type reliable information collection model. This contains an I-I/F and an proactive information cache in the agent. Managers can retrieve information for the duration the agent was unreachable, once connectivity is re-established.

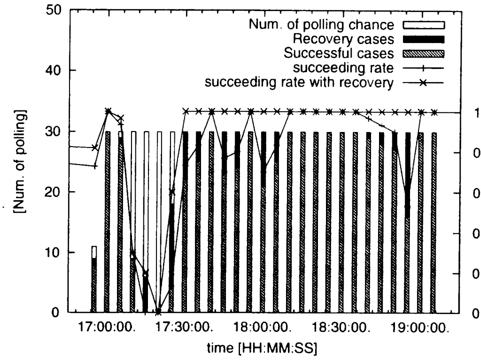

Figure 9 Polling failure rate in (Feb./12/2005 Experiment) : using proposed method.

Our implementation is based on SNMP. We have carried out experiments using the car's built-in MobileIP routers. We showed the results of monitoring GPS MIB for collecting location information from the car. We have also shown that our model is useful for online and continuous information collection tasks in real-world wireless environments.

One possible future extension of this work is to verify the data recovery rate for each type of wireless links. Optimization is necessary in data recovery to avoid any adverse effect on normal polling process.

References

[1] "Ip mobility support for ipv6" (2004). RFC 3775. [ONLINE]. Available: http://www.ietf.org/rfc/rfc3775.txt.

[2] "Mobile ipv6 management information base" (2005). draft-ietf-mip6-mipv6-mib-07.txt. [ONLINE]. Available: http://www.ietf.org/internet-drafts/draft-ietf-mip6-mipv6-mib-07.txt.

[3] "Simple Network Management Protocol (SNMP)", RFC 1157 (1990).

[4] "Report - reseach about realization of secure wireless network environment for advanced medical care activity in local region" (2005). (In Japanese, to be published).

[5] "A wireless pda-based physiological monitoring system for patient transport", IEEE Trans. Inform. Technol. Biomed., **8**, 4, pp. 439–447 (2004).

[6] "Design of a telemedicine system using a mobile telephone", IEEE Trans. Inform. Technol. Biomed., **5**, 1, pp. 13–15 (2001).

[7] "Implementation of a wap-based telemedicine system for patient monitoring", IEEE Trans. Inform. Technol. Biomed., **7**, 2, pp. 101–107 (2003).

[8] "Network approach for physiological parameters measurement", IEEE Trans. Instrum. Meas., **54**, 1, pp. 337–346 (2005).

[9] "A seamless and proactive end-to-end mobility solution for roaming across heterogeneous wireless networks", IEEE J. Select. Areas Commun., **22**, 5, pp. 834–848 (2004).

[10] "Handoff in hybrid mobile data networks", IEEE Personal Commun. Mag., **7**, 2, pp. 34–47 (2000).

[11] "A new signaling protocol for intersystem roaming in next-generation wireless systems", IEEE J. Select. Areas Commun., **19**, 10, pp. 2040–2052 (2001).