Survey and Classification of Transport Layer Mobility Management Schemes

INVITED PAPER

Mohammed Atiquzzaman and **Abu S. Reaz**
Telecommunications and Networks Research Lab
School of Computer Science, University of Oklahoma,
Norman, OK 73019-6151, USA.
Email: {atiq,sayeem_reaz}@ou.edu

Keywords: Mobility Management, IP Diversity, Transport Layer Mobility.

Abstract— **Mobility of Internet hosts allow computing nodes to move between subnets. Mobility can be handled at different layers of the protocol stack, with network and transport layer mobility being the most widely studied. Transport layer mobility can overcome many of the limitations of network layer schemes like Mobile IP. Various approaches have been proposed to implement mobility in the transport layer. In this paper, we discuss a number of transport layer mobility schemes, classify them according to their approach, and compare them based on a number of evaluation criteria.**

I. Introduction

The Internet was originally designed for static hosts connected through wired networks. Proliferation of wireless networks has given rise to an increasing demand for mobility of hosts, resulting in various mobility management schemes. Mobility management consists of two fundamental operations: Handoff and Location Management. Handoff occurs when a mobile device changes its point of attachment while still communicating with its peer. Handoff can be implemented at different layers of the protocol stack. For example, Mobile IP (MIP) [1], MSOCKS [2] and IEEE 802.11b are network layer, transport layer, and data link layer schemes, respectively. Location management refers to the task of locating (finding the IP address) a Mobile Host (MH) in order to initiate and establish a connection by a node. A good location management scheme should provide a valid address of the MH, and be transparent to its peers.

The Internet is based on a five layer architecture: physical, data link, network, transport and application layers, with each layer having specific responsibilities. Since mobility can be managed at different layers, a natural question to answer is the layer at which mobility should be managed. Several work have revealed various weakness and strengths of mobility management at the different layers. A study done by Henderson et al. [3] have compared the suitability of a number of mobility schemes at the transport, network and data link layers.

The research reported in this paper was funded by NASA Grant NAG3-2922.

In a more recent work, Eddy [4] attempts to answer the question of which layer should handle mobility, focussing on the properties of the layers themselves instead of any particular mobility scheme. The work evaluates the characteristics of network, transport and session layers for supporting seamless handoffs, location management, and change in infrastructure. He concluded that, in order to overcome various limitations that a network layer scheme (e.g. MIP [1]) poses, transport layer mobility is the most promising scheme.

As can be seen from the above studies [3], [4], a number of researchers have proposed and studied transport layer mobility schemes. Some of the schemes simply propose techniques to migrate a connection from one point of attachment to another when the MH moves, while others propose complete schemes including handoff, connection migration and location management. All the schemes are, however, built on a common assumption: an MH should be able to use a connection without any requirement for reconnection with the end node. As the transport layer establishes an end to end connection between communicating nodes, mobility schemes at this layer puts the notion of mobility at the end nodes.

A complete mobility management scheme consists of handoff, connection migration, and location management. Evaluation criteria, thus, have to be developed to determine and compare the effectiveness of mobility schemes. In this paper, we use handoff, packet loss and delay, fault tolerance, requirement for change in network infrastructure, mobility type, support for IP diversity, security, scalability, etc. to classify the proposed mobility schemes.

From the above discussion it is clear that a number of transport layer mobility schemes have been proposed. However, the authors are not aware of any published work which compares the transport layers schemes on a common framework. The *objective* of this paper is to survey transport layer mobility management schemes and compare them under a common framework. Our *contribution* in this paper is in classifying and evaluating the schemes according to their type and mobility management techniques, and comparing the schemes.

The rest of the paper is organized as follows. Fundamental issues in mobility management are discussed in Sec. II, followed by criteria to evaluate various transport layer mobility schemes in Sec. III. A number of transport layer schemes that have been proposed in the literature are discussed in Sec. IV, followed by classification of the approaches according to type of mobility in Sec. V. A comparison of the schemes based on the evaluation criteria (discussed in Sec. III) are given in Sec. VI. Finally, concluding remarks are given in Sec. VII.

II. Fundamentals of Mobility Management

Mobility management in data networks involves changing the point of attachment, and hence the IP addresses, of a Mobile Host (MH). A change in IP address gives rise to the challenges in maintaining an uninterrupted data flow while the MH is changing its address, minimizing loss of packets, maintaining security, identification of the newer location, etc. We discuss each of these issues below.

1) **Connection Migration:** An MH acquires a new IP address when it changes its subnet. Since the old IP address is retained, a natural question to answer is how the CN will continue communicating with the MH which now has multiple IP addresses. *Connection Migration*, which involves notifying the CN about this change and migrating the connection from the old to the new address, is a possible scheme. To avoid data flow through the old address of MH, connection migration may result in a temporary *stop in the data flow* during the migration process. A *gateway* in the middle of the connection may be used to handle the connection switching. Some protocols support *multiple IP addresses* for a single MH having multiple interfaces, thus enabling a smooth transition from one interface to another when changing subnets. This is discussed in details in Sec. III.
2) **Packet Loss and Latency:** When an MH acquires a new IP address, unless the MH and the underlying protocols support multiple addresses, the MH can only be contacted via the new address. Packets destined to the MH via the old address cannot reach the destination, resulting in packet loss, latency and wastage of internet bandwidth. Mobility schemes must come up with techniques to mitigate packet losses and latency during handoffs.
3) **Infrastructure Requirement:** The Internet was not initially designed with mobility in mind. Consequently, many of the proposed schemes require changes in the existing Internet infrastructure, such as gateway or proxy in the middle of the connection, to support mobility.
4) **Location Management:** Following the change of IP address of an MH, a CN should be able to locate the MH. A location manager keeps track of the current IP address of an MH, and provides the current address to any entity trying to initiate communication with the MH.

In this section, we have discussed the issues to be considered in designing a mobility management scheme. In the next section, we discuss various criteria that can be used to evaluate and compare mobility management schemes based on the issues discussed in this section.

III. Evaluation Criteria

In this section, we define a set of evaluation criteria which will be used to compare the various mobility schemes in Sec. VI. We first describe a generic handoff scenario and related issues which will help us in determining the relevant evaluation criteria.

When an MH decides to detach itself from one subnet and connect to another one based on the signal strength of neighboring subnets, the MH obtains a new IP address from the new subnet. The data already in transit to the MH's old IP address may be lost, resulting in increased delay due to retransmission of the lost packets. The change in point of attachment may be confined to a single subnet or a group of neighboring subnets. The handoff may require applications running on MH and CN to be aware of mobility, thereby reducing application transparency. Additionally, handoff between subnets may also result in conflict with standard network security solutions, and may require additional hardware/software to be deployed in the existing network infrastructure. Based on this handoff scenario, we define the following evaluation criteria for mobility schemes.

1) **Handoff Process:** The performance of a mobility management scheme depends on the type of handoff [5] which can be either soft or hard. *Soft handoff* (also called seamless handoff) permits a smooth handoff by allowing a mobile to communicate and exchange data with multiple interfaces simultaneously during handoff. Communication through the old interface is dropped when the signal strength from the corresponding access point drops below a certain threshold. On the contrary, *hard handoff* results in disconnecting from the old access point when the signal strength is below a threshold before connecting to the new access point.
2) **Scalability and Fault Tolerance:** Scalability refers to the ability of a mobility management scheme to handle a large number of MHs and CNs. A scheme is scalable when its performance does not drop with an increase in the size of the network size or the number of MHs and CNs. A system is said to be fault tolerant when it can function in the presence of system failures. For example, a scheme with a single point of failure in said to be fault intolerant.
3) **Application Transparency:** A mobility scheme is transparent to an application when the application does not need to know about handoff taking place in the lower layers, and hence does not require any modification to the application.
4) **Loss/Delay:** Packets in flight may not be delivered to the MH during the handoff period. This may result in packet losses, packet delay, and a false indication of congestion in the network.
5) **Security Solutions:** Internet is vulnerable to many security threats. Many of the solutions, such as ingress filtering and firewalls, to the threats do not allow network entities to process packet headers as may be required by

some of the mobility schemes.

6) **Path Diversity/IP Diversity:** Increasing number of mobile devices nowadays come with multiple communication interfaces. During handoff, an MH may be able to take advantage of multiple IP addresses (called IP diversity), obtained from separate subnets, associated with the multiple interfaces.
7) **Change in Infrastructure:** A mobility management scheme may require additional software agents (such as Home/Foerign agents in the case of MIP) or hardware to be deployed in the existing network infrastructure. Such additional agents/hardware may result in scalability and deployment issues for the scheme to be implemented in the real world.
8) **Change in Protocol:** A transport layer mobility management scheme may require change in the transport protocol, or may require applications to use a new transport protocol or API.

We use the various criteria for evaluation of mobility management schemes discussed in this section for evaluating, comparing, and classifying different transport layer schemes (Sec. IV) in Sec. V.

IV. Transport Layer Schemes

In this section, we discuss a number of transport layer schemes that have been proposed in the literature. While Mobile IP is a network layer scheme which makes mobility transparent to upper layers by increasing the burden and responsibility of the Internet infrastructure, transport layer schemes are based on an end-to-end approach to mobility that attempt to keep the Internet infrastructure unchanged by allowing the end hosts to take care of mobility.

A. MSOCKS

Maltz et al. [6] propose TCP Splice to split a TCP connection at a proxy by dividing the host-to-host communication into host-proxy and proxy-host communications. MSOCKS [2] uses TCP Splice for connection migration (Sec. II) and supports multiple IP addresses for multiple interfaces. When an MH disconnects itself from a subnet during handoff, it obtains a new IP address from the new subnet using DHCP, and establishes a new connection with the proxy using its second interface. The communication between proxy and CN, however, remains unchanged. The data flow between MH and CN thus continues, with the CN being unaware of the mobility. Location management is done through the proxy which is always aware of the location of the MH; this limits the mobility within the coverage of the proxy.

B. SIGMA

Seamless IP diversity based Generalized Mobility Architecture (SIGMA) [7] is a complete mobility management scheme implemented at the transport layer, and can be used with any transport protocol that supports IP diversity. SIGMA supports IP diversity-based soft handoff. As an MH moves into the overlapping region of two neighboring subnets, it obtains a new IP address from the new subnet while still having the old one as its primary address. When the received signal at the MH from the old subnet goes below a certain threshold, the MH changes its primary address to the new one. When it leaves the overlapping area, it releases the old address and continues communicating with the new address thus achieving a smooth handoff across subnets. Location management in SIGMA is done using DNS [8] as almost every Internet connection starts with a name lookup. Whenever an MH changes its address, the DNS entry is updated so that subsequent requests can be served with the new IP address.

C. Migrate

Migrate [9] is a transparent mobility management scheme which is based on connection migration using Migrate TCP [9], and uses DNS for location management (Sec. II). In Migrate TCP, when an MH initiates a connection with a CN, the end nodes exchange a token to identify the particular connection. A hard handoff (Sec. III) takes place when the MH reestablishes a previously established connection using the token, followed by migration of the connection. Similar to SIGMA (Sec. IV-B), this scheme proposes to use DNS for location management.

D. Freeze-TCP

Freeze-TCP [10] is a connection migration scheme (Sec. II) that lets the MH 'freeze' or stop an existing TCP connection during handoff by advertising a zero window size to the CN, and unfreezes the connection after handoff. This scheme reduces packet losses during handoff at the cost of higher delay. Although it provides transparency to applications, Freeze TCP requires changes to the transport layer at the end nodes. Freeze-TCP only deals with connection migration, but does not consider handoff or location management. It can be employed with some other schemes like Migrate (Sec. IV-C) to implement a complete mobility management scheme.

E. R^2CP

Radial Reception Control Protocol (R^2CP) [11] is based on Reception Control Protocol (RCP), a TCP clone in its general behavior but moves the congestion control and reliability issues from sender to receiver on the assumption that the MH is the receiver and should be responsible for the network parameters. R^2CP has some added features over RCP like the support of accessing heterogenous wireless connections and IP diversity that enables a soft handoff (Sec. III) and bandwidth aggregation using multiple interfaces. A location management scheme might be integrated with R^2CP to deploy a complete scheme.

F. MMSP

Mobile Multimedia Streaming Protocol (MMSP) [12] supports transparent soft handoff through IP diversity (Secs. II and III) and uses bicasting (a technique to duplicate a flow simultaneously) to prevent losses during the handoff period. This protocol uses Forward Error Correction (FEC) and fragmentation to mitigate wireless errors and does not include location management.

G. I-TCP

Indirect TCP (I-TCP) [13] is a mobility scheme that requires a gateway (Sec. II) between the communication path of the CN and MH to enable mobility. In this scheme, a TCP connection between CN and gateway and a I-TCP connection between the gateway and MH is established to provide CN to MH communication. The TCP portion remains unchanged during the lifetime of the communication and remains unaware of the mobility of MH. In the I-TCP portion, when the MH moves from one subnet to another one, a new connection between MH and the gateway is established and the old one is replaced by the new one. The transport layer of the MH needs to be modified but applications enjoy a transparent view of the mobility at both the ends. I-TCP does not support IP diversity and soft handoff. Location management is not included in this scheme.

H. M-TCP

Mobile TCP (M-TCP) [14], an enhanced version of I-TCP (Sec. IV-G), is implemented at MH which works like a link layer one hop protocol that connects to the gateway via wireless. The gateway maintains a regular TCP connection with the CN and redirects all packets coming from CN to MH. This redirection is unnoticed by both the MH and CN. The enhancement of M-TCP over I-TCP is in requiring less complexity in the wireless part of the connection. Similar to I-TCP, M-TCP does not support IP diversity or location management but ensures transparency to applications.

I. M-UDP

Mobile UDP (M-UDP) [15] is an implementation of UDP protocol with mobility support similar to I-TCP and M-TCP (Secs. IV-G and IV-H). Like M-TCP, M-UDP uses a gateway to split the connections between MH and CN to ensure one unbroken gateway to CN connection and continuously changing MN to gateway connection. This also does not include IP diversity or location management.

J. BARWAN

The Bay Area Research Wireless Access Network (BARWAN) [16] is a solution to heterogenous wireless overlay network. It has a gateway centric architecture (Sec. II) on an assumption that the wireless networks are built around the gateways. Diverse overlapping networks are integrated through software that operates between the MH and the network. This supports the MH to move among multiple wireless networks - whenever MH moves out of a lower coverage network (e.g. WLAN) it moves into a higher coverage network (e.g. WWAN) and MH changes its connection from lower to higher one. This scheme supports IP diversity for the MH hence enables seamless handoff across different networks. BARWAN requires the application to be aware of mobility as the decision to make a handoff is taken by the application. This scheme does not specify a location manager.

K. TCP-R

TCP Redirection (TCP-R) [17] is a connection migration scheme that maintains active TCP connections during handoff (Sec. III) by updating end-to-end address pairs. Whenever MH gets a new IP address, TCP-R updates the address at CN and the already existent connection continues with the new address. TCP-R does not implement connection timeout to support long disconnection. Transport layer at both the ends needs modification for this support, yet it gives application transparency. Like Migrate (Sec. IV-C), TCP-R proposes to use DNS as location manager. Combined with a handoff management scheme, this scheme might be deployed as a complete mobility scheme.

L. mSCTP

Mobile SCTP (mSCTP) [18] supports IP diversity and soft handoff (Sec. III). The handoff is similar to the one of SIGMA (Sec. IV-B). mSCTP can maintain application transparency but it does not support location management.

M. Miscellaneous

There are a few more protocols and schemes that have the potential to support (e.g. MTCP [19] is a TCP based transport protocol that supports live connections to seamlessly migrate servers) or improve performance of mobility (e.g. pTCP [20] supports IP diversity and can achieve bandwidth aggregation of wireless networks through multiple interfaces) schemes. Since they have not been proposed as mobility schemes, we do not discuss them in this paper.

V. Classification of transport layer schemes

The mobility management schemes described in Sec. IV can be classified, based on their approach towards mobility, into four groups as shown in Table I and described below.

1) **Handoff Protocol:** Rather than being complete mobility management schemes, schemes belonging to this class are enhancements of transport layer protocols that aim at improving the performance, such as low latency and reduced data loss, of mobile hosts during handoff. This class consists of R^2CP, MMSP and mSCTP (Sec. IV), each of which supports IP diversity and seamless handoff. They can aid handoff, but are not complete mobility management schemes because of their lack of mobility management components, such as location management.
2) **Connection Migration Protocol:** The mobility schemes is this class are based on migrating connections which have been stopped or put under waiting (Sec. II) during handoff in order to ensure a single unbroken connection between CN and MH. They do not deal with handoff issues. Examples are Freeze-TCP and TCP-R (Sec. IV) which are enhancements of TCP to allow a connection to be stopped and restarted before and after a handoff, respectively.

TABLE I

TRANSPORT LAYER MOBILITY SCHEMES CLASSIFIED BY APPROACH

Class	Description	Example
Handoff protocol	Transport Layer Protocol that has features to support mobility	R^2CP, MMSP and mSCTP
Connection migration protocol	Transport Layer Protocol that can migrate multiple connections	Freeze TCP and TCP-R
Gateway-based mobility scheme	Provides mobility by putting a infrastructure between CN and MH and splitting the connection	MSOCKS, I-TCP, M-TCP, M-UDP and BARWAN
Mobility manager	Complete mobility schemes with handoff and location management	Migrate and SIGMA

3) **Gateway based Mobility Scheme:** Schemes in this class handle mobility with a special gateway in the Internet infrastructure (change in infrastructure in Sec. II). The connection between CN and MH is split at the gateway, with the connection between the gateway and CN being fixed while allowing the MH to roam and change its connection with the gateway. MSOCKS, I-TCP, M-TCP, M-UDP and BARWAN (Sec. IV), which belong to this class, requires special entities that split the connection between the MH and CN. The do not provide details about implementation of location managers, and hence are not complete mobility management schemes.
4) **Mobility Management:** Schemes in this class provide complete end to end mobility management schemes at the transport layer. Migrate and SIGMA (Sec. IV), which belong this group, provide complete end-to-end mobility management schemes by implementing handoff and location management.

In the next section, we compare among the schemes belonging to a particular class.

VI. COMPARISON WITHIN CLASSES

In the previous section, we have classified the mobility schemes in to four classes. Since it is not fair to individually compare mobility schemes belonging to different classes, in this section, we compare between mobility schemes belonging to the same class using the criteria discussed in Sec. III.

A. Handoff Protocols

Table II provides a detailed comparison between the protocols in this class, viz. R^2CP, MMSP and mSCTP, which support IP diversity, allowing a possibility of soft handoff and low packet loss during handoff. R^2CP receiver centric in terms of maintaining the congestion control parameters. Since most MHs are assumed to be clients (i.e. receivers), having the congestion control at the mobility-aware receiver results in better performance in terms of throughput and delay by being able to distinguish between mobility and corruption related losses. However, there is a risk of the performance degradation if the MH plays the role of a server.

All the schemes in this class are transport layer protocols which handle mobility, and hence, provide application layer transparency. The schemes are based on end-to-end protocols, and hence are scalable and fault tolerant. The schemes in this class do not require packet headers to be processed by the network; they can thus work with standard security solutions.

TABLE II

COMPARISON AMONG HANDOFF PROTOCOLS

Criteria	R^2CP	MMSP	mSCTP
Handoff	Soft	Soft	Soft
Fault tolerance	Yes	Yes	Yes
Transparency	Yes	Yes	Yes
Loss/Delay	If MH is the server	Prevents	Prevents
Conflicts with security solution	No	No	No
IP Diversity	Supports	Supports	Supports
Change in infrastructure	No	No	No
Change in protocol stack	Yes	Yes	Yes

TABLE III

SUMMARY OF CONNECTION MIGRATION PROTOCOLS

Criteria	TCP Freeze	TCP-R
Handoff	N/A	N/A
Fault tolerance	Yes	Connection teardown would go to infinite wait
Transparency	Yes	Yes
Loss /Delay	Avoids data transfer during handoff to prevent loss	On the fly packets are lost
Conflicts with security solution	No	No
IP Diversity	No	No
Change in infrastructure	No	No
Change in protocol stack	No in CN, Yes in MH	Yes

B. Connection Migration Protocols

Table III gives a brief description and comparison of Freeze TCP and TCP-R which are connection migration protocols that support long and frequent disconnections during handoff, resulting in fewer packet losses. Freeze TCP requires changing the TCP protocol stack only at the MH, whereas the protocol stacks at both the MH and CN have to be changed in the

TABLE IV

SUMMARY OF GATEWAY-BASED MOBILITY SCHEMES

Criteria	MSOCKS	I-TCP	M-TCP	M-UDP	BARWAN
Handoff	Hard	Hard	Hard	Hard	Soft
Fault tolerance	Single point of failure: proxy	Single point of failure: gateway	Single point of failure: gateway	Single point of failure: gateway	Single point of failure: gateway
Transparency	Yes	Yes	Yes	Yes	No
Loss /Delay	On the fly packets are lost	On the fly packets are lost	On the fly packets are lost	On the fly packets are lost	Prevents
Conflicts with security solution	Yes	Yes	Yes	Yes	Yes
IP Diversity	No	No	No	No	Supports
Change in infrastructure	Yes	Yes	Yes	Yes	Yes
Change in protocol stack	Yes at MH, no at CN	Yes at MH, no at CN	Yes at MH, no at CN	Yes at MH, no at CN	Yes

case of TCP-R. The change in the transport layer is, however, transparent to applications, and do not require any change to the existing network infrastructure. Both Freeze TCP and TCP-R use TCP which does not support IP diversity, and hence requires hard handoff. Unlike proxy based schemes, the protocols do not require any packet header processing in the network, and hence work well with security solutions in the network. None of these schemes has a single point of failure, but TCP-R does not implement connection timeout, and hence risks of going into infinite wait in case of connection teardown.

C. Gateway-based Mobility Scheme

Table IV summarizes five mobility schemes, viz. MSOCKS, I-TCP, M-TCP, M-UDP and BARWAN, which require a gateway to be implemented in the network for handling mobility. Packet header processing at the gateway may interfere with security solutions (such as IPSec). Moreover, use of a gateway poses a single point of failure and may give rise to fault tolerance issues.

The use of connection splicing at the gateway by MSOCKS, I-TCP, M-TCP, and M-UDP may result in loss of in-flight packets during handoff, and packet delays resulting from retransmission of lost packets. Handling of the mobility at the transport layer makes these four schemes transparent to the applications, and requires change of the protocol stack at MH only. In contrast, applications in BARWAN initiate handoff and hence makes mobility non-transparent to applications. Unlike other schemes in this class, BARWAN supports soft handoffs by using IP diversity.

D. Mobility Managers

Table V presents a comparison of Migrate and SIGMA which provide complete mobility management schemes including handoff and location management, and are therefore classified as mobility managers. These schemes do not use any special network infrastructure; hence, they are compliant with standard network security solutions. Both SIGMA and Migrate require changes in transport layer but maintain application transparency.

In contrast to SIGMA which does not suffer from packet loss, Migrate may loose in flight packets during handoff. Neither of them requires any change in Internet infrastructure, but Migrate requires change in TCP. Neither of these schemes have a single point of failure although new connection requests carry the potential risk of failure if LM fails.

TABLE V

SUMMARY OF MOBILITY MANAGERS

Criteria	Migrate	SIGMA
Handoff	Hard	Soft
Fault tolerance	New connections would fail if location manager fails	New connections would fail if location manager fails
Transparency	Yes	Yes
Loss /Delay	No, but stops transmission	No
Conflicts with security solution	No	No
IP Diversity	No	Supports
Change in infrastructure	No	No
Change in protocol stack	Yes	Yes

E. Summary of Comparison between Classes

Based on the evaluation criteria defined in Sec. III, Table VI depicts a comparison between the classes described in Sec. V. All the schemes in the handoff protocol class (Sec. VI-A) support soft handoff through IP diversity, and hence avoid packet loss. Schemes in the connection migration class (Sec. VI-B), on the other hand, do not support IP diversity and soft handoff, and thus suffer packet loss during handoff. Freeze-TCP, however, mitigates packet losses by stopping the connection during handoff at the expense of packet delays during handoff. Apart from BARWAN, the gateway-based mobility schemes (Sec. VI-C) do not implement soft handoff due to a lack of support for IP diversity, and hence, suffer loss during connection migration. SIGMA is the only scheme in the mobility manager class (Sec. VI-C) which eliminates packet losses during handoff through IP diversity-based soft handoff.

Only the schemes in the gateway based mobility class require changes in existing Internet infrastructure, thereby

TABLE VI

SUMMARY OF TRANSPORT LAYER SCHEMES

Criteria	Handoff Protocols	Connection Migration Protocols	Gateway based Mobility Scheme	Mobility Managers
Handoff	Soft	N/A	Usually hard, soft for BARWAN	Soft, hard for Migrate
Fault tolerance	Yes	Yes	Fails if infrastructure fails	New connections would fail if location manage fails
Transparency	Yes	Yes at CN, No at MH	Usually Yes, No for BARWAN	Yes, No for Migrate
Loss /Delay	No	On the fly packets are lost for R-TCP, Freeze-TCP prevents loss	On the fly packets are lost, No for BARWAN	No, Migrate stops transmission
Conflicts with security solution	No	No	Yes	No
IP Diversity	Supports	No	No, Supports for BARWAN	Supports, No for Migrate
Change in infrastructure	No	No	Yes	No
Change in protocol stack	Yes	Yes	Yes	Yes

creating a single point of failure. These schemes also conflict with generic security solutions as they require packet header processing by the gateways. Rest of the schemes can be implemented without any physical change in the existing network infrastructure, and hence do not introduce any vulnerability due to a single point of failure or conflict with security solutions.

As all the schemes described in this paper handle mobility at the transport layer, they require changes in the transport layer of the protocol stack. Nonetheless, apart from BARWAN in which applications initiate handoff, all the schemes keep the applications transparent from mobility.

VII. CONCLUSION

In this paper, we have provided a comprehensive survey and classification of mobility management schemes at the transport layer. Transport layer-based schemes enjoy several advantages that motivated researchers to propose different schemes to manage mobility at the transport layer. As far as the authors are aware, this is the first paper which provides a comprehensive overview, classification and comparisons of transport layer based mobility schemes. We conclude that a complete mobility scheme that supports IP diversity and soft handoff, transparency to applications, and can be deployed without any change in the network infrastructure is very suitable for handling mobility of hosts in the Internet.

REFERENCES

[1] C. Perkins, "IP mobility support." IETF RFC 3344, August 2002.

[2] D. A. Maltz and P. Bhagwat, "MSOCKS: an architecture for transport layer mobility," *IEEE INFOCOM*, San Francisco, CA, pp. 1037 – 1045, March 29 - April 2, 1998.

[3] T. R. Henderson, "Host mobility for IP networks: a comparison," *IEEE Network*, vol. 17, no. 6, pp. 18 – 26, Nov - Dec 2003.

[4] W. M. Eddy, "At what layer does mobility belong?," *IEEE Communications Magazine*, vol. 42, no. 10, pp. 155 – 159, October 2004.

[5] N. D. Tripathi, J. H. Reed, and H. F. VanLandinoham, "Handoff in cellular systems," *IEEE Personal Communications*, vol. 5, no. 6, pp. 26 – 37, December 1998.

[6] D. Maltz and P. Bhagwat, "TCP splicing for application layer proxy performance," IBM Research Report RC 21139, IBM T.J. Watson Research Center, March 1998.

[7] S. Fu, L. Ma, M. Atiquzzaman, and Y. Lee, "Architecture and performance of SIGMA: A seamless handover scheme for data networks," *IEEE ICC*, Seoul, South Korea, May 16-20, 2005.

[8] A. S. Reaz, M. Atiquzzaman, and S. Fu, "Performance of DNS as Location Manager," *IEEE Electro/Information Technology Conference*, Lincoln, NE, May 22-25 2005.

[9] A. C. Snoeren and H. Balakrishnan, "An end-to-end approach to host mobility," *MOBICOM*, Boston, MA, pp. 155 – 166, August 6-11, 2000.

[10] T. Goff, J. Moronski, D. S. Phatak, and V. Gupta, "Freeze-TCP: a true end-to-end TCP enhancement mechanism for mobile environments," *IEEE INFOCOM*, Tel Aviv, Israel, pp. 1537 – 1545, March 26-30, 2000.

[11] H. Hsieh, K. Kim, Y. Zhu, and R. Sivakumar, "A receiver-centric transport protocol for mobile hosts with heterogeneous wireless interfaces," *ACM MobiCom*, San Diego, CA, pp. 1 – 15, September 14-19, 2003.

[12] H. Matsuoka, T. Yoshimura, and T. Ohya, "End-to-end robust IP soft handover," *IEEE ICC*, Anchorage, Alaska, pp. 532 – 536, May 11-15, 2003.

[13] A. Bakre and B. R. Badrinath, "I-TCP: indirect TCP for mobile hosts," *IEEE International Conference on Distributed Computing Systems*, Vancouver, Canada, pp. 136 – 143, May 30 - June 2, 1995.

[14] Z. J. Haas and P. Agrawal, "Mobile-TCP: an asymmetric transport protocol design for mobile systems," *IEEE ICC*, Montreal, Canada, pp. 1054 – 1058, June 8 - 12, 1997.

[15] K. Brown and S. Singh, "M-UDP: UDP for mobile cellular networks," *Computer Communication Review*, vol. 26, no. 5, pp. 60 – 78, October 1996.

[16] R. H. Katz, E. A. Brewer, E. Amir, H. Balakrishnan, A. Fox, S. Gribble, T. Hodes, D. Jiang, G. T. Nguyen, V. Padmanabhan, and M. Stemm, "The bay area research wireless access network (BARWAN)," *IEEE COMPCON*, Santa Clara, CA, pp. 15 – 20, February 25-28, 1996.

[17] D. Funato, K. Yasuda, and H. Tokuda, "TCP-R: TCP mobility support for continuous operation," *IEEE International Conference on Network Protocols*, Atlanta, GA, pp. 229 – 236, October 28 - 31, 1997.

[18] S.J. Koh, M. J. Chang, and M. Lee, "mSCTP for soft handover in transport layer," *IEEE Communications Letters*, vol. 8, no. 3, pp. 189 – 191, March 2004.

[19] F. Sultan, K. Srinivasan, D. Iyer, and L. Iftode, "Migratory TCP: connection migration for service continuity in the internet," *IEEE International Conference on Distributed Computing Systems*, Vienna, Austria, pp. 469 – 470, July 2002.

[20] H. Hsieh and R. Sivakumar, "pTCP: an end-to-end transport layer protocol for striped connections," *IEEE International Conference on Network Protocols*, Paris, France, pp. 24 – 33, November 12-15, 2002.