TRUST-BY-WIRE IN PACKET-SWITCHED NETWORKS: CALLING LINE IDENTIFICATION PRESENTATION FOR IP

Stephan Kubisch, Harald Widiger, Peter Danielis, Jens Schulz, Dirk Timmermann

University of Rostock
Institute of Applied Microelectronics and Computer Engineering
18051 Rostock, Germany
Tel./Fax: +49 (381) 498-7276 / -1187251
{stephan.kubisch;harald.widiger}@uni-rostock.de
http://www.imd.uni-rostock.de/networking

*Daniel Duchow, Thomas Bahls**

Nokia Siemens Networks GmbH & Co. KG
Broadband Access Division
17489 Greifswald, Germany
Tel./Fax: +49 (3834) 555-642 / -602
{daniel.duchow;thomas.bahls}@nsn.com
http://www.nokiasiemensnetworks.com

ABSTRACT

During the last decades, the Internet has steadily developed into a mass medium with millions of users. On the one hand, newfangled services replace traditional ones. Naturally, these are thereby expected to offer at least the same features as their classical pendants, e.g., when VoIP replaces traditional fixed line telephone networks. On the other hand, the requirements on network infrastructures and services have changed. A reason for that is the lack of Trust-by-Wire *in packet-switched IP networks. In traditional telephone networks, a phone number directly coheres with a physical line. This direct relationship is* not *given in modern packet-switched IP networks. An IP address does not identify a physical line! This paper presents a new mechanism, which guarantees Trust-by-Wire in packet-switched IP networks—called* Internet Protocol-Calling Line Identification Presentation (IPclip). *Unambiguous and trustworthy location information is added on the IP level. Firstly, IPclip's general functionality is presented. Secondly, we discuss IPclip in the light of location-aware emergency calls in nomadic VoIP environments.*

Index Terms— Internet Protocol, Network Operation, VoIP, Mobility, Emergency Services

1. INTRODUCTION

As the original Internet has grown from a pure scientific network into a world-wide communication medium [1], the requirements towards network infrastructures and provided services have changed radically. Besides the advantages of using the Internet for business, communication, and information retrieval, it also has its "dark sides" like security issues, complexity, and anonymity. This has—among others—the following reasons:

- The Internet's complexity and therewith the anonymity of users are increasing. Once, the Internet was an environment where every party could be considered as trustworthy. Today, loopholes are exploited to hide identity.
- Aged protocols, which have originally *not* been designed for such a large community [2], show shortcomings. Nobody could foresee backdoors and security risks.
- Packet-switched networks do lack inherent *Trust-by-Wire*. This is due to the fact that in classical circuit-switched networks, e.g., PSTN, a phone number directly references to a fixed line. Whereas this direct interrelationship is not given in packet-switched networks like the Internet.

Furthermore, new services replace conventional systems, e.g., VoIP, which will replace classical fixed line telephone networks soon. But VoIP would not be an improvement if it does not provide at least the same features. Naturally, customers expect new services to offer at least the same features and Quality-of-Service as the conventional techniques. Regarding VoIP, emergency calls (ECs) are a hot topic [3, 4]. One key

*We would like to thank the Broadband Access Division of Nokia Siemens Networks in Greifswald, Germany for their inspiration and continued support in this project. This work is partly granted by Nokia Siemens Networks.

advantage with VoIP is mobility and nomadic use to be reachable and have service from any place at any time. However, high mobility poses the problem of providing precise location information (LI) of the caller, which is vital information in case of ECs. But the Trust-by-Wire model is *not* given in mobile VoIP environments as well as in other packet-switched IP networks. For fixed telephone lines, the location of the terminals is well known. But for VoIP, this is not the case. Even if a subscriber device possessed a unique IP address and access port number, this is not sufficient to physically locate a caller. Neither do IP addresses provide the same geographic unambiguousness as phone numbers nor have IP addresses been designed for specific purposes like mobile services [3]. Thus, without trustworthy references to a caller's position, an EC cannot be directed to the responsible Public Safety Answering Point (PSAP) to locate and help the caller. Currently, there is no standard that harmonizes nomadic VoIP ECs but only best practices [5]. Consequently, a manageable solution to provide trustable and accurate LI is required in packet-switched IP networks, e.g., to determine the caller's position for a VoIP EC.

In this paper, we address the latter of the reasons mentioned above—Trust-by-Wire in packet-switched IP networks. We present a new mechanism called *Internet Protocol-Calling Line Identification Presentation (IPclip)*. It associates trustworthy information about the IP packets' origin in form of IP options. This information is added at the ingress points of the access networks. IPclip itself is a generic mechanism, which is totally decoupled from specific applications. VoIP ECs are thus used as use case to exemplify the IPclip mechanism and the Trust-by-Wire framework.

2. THE IPCLIP MECHANISM IN GENERAL

The name IPclip is derived from the CLIP function of Integrated Services Digital Networks (ISDN). Originally, CLIP is used as an optional feature in ISDN telephone networks. With CLIP, the number of the caller is transmitted to the callee allowing precise identification of the caller. In case of IP, a user's IP address *cannot* be considered as equivalent to a phone number, because an IP address does not uniquely reference a physical line. Furthermore, IP addresses *do not* provide LI in any case whereas phone numbers *do have* a well-defined origin. Therefore, IPclip reuses selected, principle aspects of the ISDN CLIP function in IP-based packet-switched networks to facilitate enhanced and new services.

With the IPclip mechanism, a customer and his actual geographic location are identified using a tuple, which consists of the current IP address and extra information. While the IP address might identify a user, his position must be part of the additional data. Preferably, a standardized format of LI is used. It can be interpreted for analysis, for classification, for generation of syslog-calls to induce further exceptional actions, or to send help to a person that requires medical assistance in case of VoIP ECs.

To provide such LI on a global scale, IPclip inserts it as IP option into every IP packet in the upstream data path. IP spans the whole Internet and provides end-to-end connectivity. Structure and size of IP options are standardized. Thus, by using IP options, IPclip is a standard-compliant solution to convey extra information. IP options as part of the IP header can have a maximum length of 40 bytes that can contain arbitrary additional information [6]. Thereby, network devices can either process this IP option or ignore it. But in any case, devices must be capable of parsing the complete IP header for reasons of interoperability. Furthermore, the IPclip system provides the option to remove existing LI from IP packets in the downstream data path to not forward LI to the end-user.

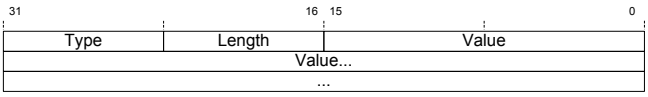

Fig. 1. TLV format of an IP option

The addition of LI, including its verification and signaling of the verification result, relates to certain major aspects:

- What is the format of the additional LI?
- Which is the place within the network infrastructure where the LI is available?
- Which is the place in the network where this LI can be added to IP packets?
- How can a trust relationship and some degree of credibility be described and how can it be ensured when validating the LI?
- By adding additional bytes to packets, the Maximum Transmission Unit (MTU) may be exceeded and needs to be adapted.

2.1. IPclip Option Format

The IPclip option and the LI are one possible value for an IP option. It must not be mixed up with an IP option!

2.1.1. IP Options

As specified in RFC 791 [6], an IP option can either consist of one byte that represents the option or a multiple of four bytes that are structured as shown in Figure 1. This format is commonly known as Type-Length-Value (TLV) structure. Details on the single fields can be derived from the RFC.

Although the IPclip system provides mechanisms to prevent fragmentation, the Copied-Flag in the IP options TLV should be set so that LI is copied on to all fragments if fragmentation does occur. Option class should be set to 0 (control) because the framework envisages the regular implementation into systems. At the moment, 26 is chosen as IP option number for the IPclip prototype since it is currently not in use [7].

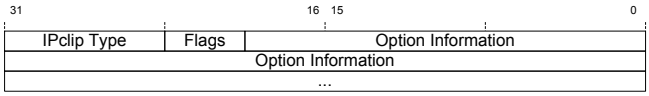

Fig. 2. Format of an IPclip option

2.1.2. *IPclip Options*

The IPclip option is inserted *in the value field of a TLV-structured IP option*. It allows for transmission of arbitrary information. As shown in Figure 2, the IPclip option consists of 1 byte for the IPclip type, 4 bit for flags, and the option information of variable size. Padding may be necessary to the next multiple of four bytes less one byte to resize the total IP option to a multiple of four bytes.

Table 1 shows the possible values for the IPclip option type. The values 0 and 31 are reserved. Approved geographic standards, which are well-known in the field of geographic information systems, are used for the IPclip LI. Value 1 denotes Global Positioning System (GPS) [8]. Value 2 denotes Geospatial Location Information (GLI) [9]. Values 3 and 4 refer to GPS or GLI plus access node ID and access port information. This tuple of information allows for more precise localization of the user. Other values have not been assigned yet.

Table 1. IPclip option types

Value	Type Description
0 & 255	reserved
1	GPS
2	GLI
3	GPS + Access Node ID & Port Number
4	GLI + Access Node ID & Port Number
5...254	unused

4 bits are designated for status flags. 2 bits define source and credibility of the IPclip option as already sketched in Table 3. The remaining 2 bits are reserved for future use.

Table 2. GPS Location Information Format

Information	Range	# of bits
Option Information		57
Latitude		28
Degree	0...90	7
Minutes (Integer)	0...90	6
Minutes (Fraction)	0...(1-2^{-15})	14
Hemisphere	N, S	1
Longitude		29
Degree	0...180	8
Minutes (Integer)	0...59	6
Minutes (Fraction)	0...(1-2^{-15})	14
Hemisphere	E, W	1

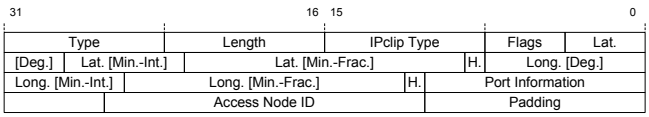

Fig. 3. IP option containing an IPclip option with GPS-formatted LI, access node ID, and port number

2.1.3. *GPS and Geospatial Location Information*

The data format, which is used for the conveyance of GPS information, is the NMEA-0182 data format [8]. Information that is relevant for the IPclip option contains latitude and longitude (see Table 2). A possible encoding for the whole IP option is illustrated in Figure 3. A complete encoding requires at least 57 bits. With 12 bit for IPclip type and flags, this results in 9 bytes for the IPclip option. For the complete TLV-structured IP option, 11 bytes are needed. Adding port information and access node ID, the IPclip option's total length increases to 15 bytes including IPclip-padding. This way, the complete IP option is 16 bytes in length to conform to a multiple of 4.

This is analogous for GLI-formatted LI [9], which may also include the altitude.

2.2. IPclip's Position within the Network Infrastructure

Network ingress—known as access network—is considered as the most reasonable place where LI can be added and verified. Access networks comprise Customer Premises Equipment (CPE) as well as so-called access nodes (ANs) like IP DSL Access Multiplexers. Usually, access nodes consist of multiple linecards and an aggregation card. Aggregation cards manage high-bandwidth interfaces towards the core network. Linecards mainly concentrate high numbers of subscribers. This structure is shown in Figure 4.

The inherent physical line information, e.g., the access port number on the AN, can already be treated as some flavor of LI. Thus, our approach is based on the assumption that LI can be added either by the CPEs (only IPclip option type 1) or by the IPclip mechanism in the ANs (IPclip option type 3). However, verification and validation of the LI and thereupon taken measures are solely done in the ANs. The reason for doing so is that CPEs are typically not considered

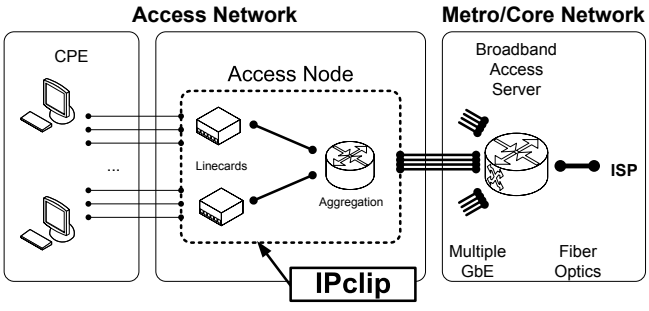

Fig. 4. Access network with IPclip

Table 3. IPclip option flags

Flags	Source / Credibility	Option Description
00	user provided/ untrusted	A user provided IPclip option did not pass validation.
01	user provided/ trusted	A user provided IPclip option did pass validation.
10	network provided/ untrusted	A User provided IPclip option did not pass validation and is replaced.
11	network provided/ trusted	A new IPclip option is added on the AN.

as trustworthy network elements. CPEs are usually not within the carriers' or ISPs' management domains. By contrast, ANs are part of the access network and thus within a carrier's management domain. A tuple of information available in ANs is used as precise LI to identify and locate a user:

- The accurate geographic location of the AN
- The access port number of the user
- The access node ID

That is why the IPclip functionality is implemented on ANs as highlighted in Figure 4.

2.3. Trust and Credibility

IPclip recognizes user provided IPclip options. But due to mobility, reasons of misconfiguration, or even intentional concealment of the packets' true origin—CPE is not trustworthy—it needs to be validated. IPclip can identify incorrect LI to a certain degree. Only customers locally near to a specific AN can be connected to it. This area is called *Subscriber Catchment Area* (SCA) of the respective AN. The plausibility of the user provided LI is validated by comparing it with the hard-coded LI of the AN and its SCA. Thereby, incorrect LI is replaced with the inherent LI of the AN. The replacement of incorrect information ensures valid LI at any time, which provides at least the accuracy of the location of the originating AN. Additionally, two flags are set as result of the validation procedure. These flags serve as additional triggers in specific application scenarios as, e.g., described in Section 4. Table 3 briefly summarizes the interpretation of the status flags. The trust relationship is preserved by these flags at any time since they are assigned in the network carrier's management domain. The naming convention for these flags has been adapted to the commonly used lingo in the area of communication technology.

Each incoming packet is inspected for existing IPclip options. If a defined and valid LI format is used, e.g., GPS or GLI, the LI is read and compared with the AN's own LI. Thereby, a logical square is spanned surrounding the access

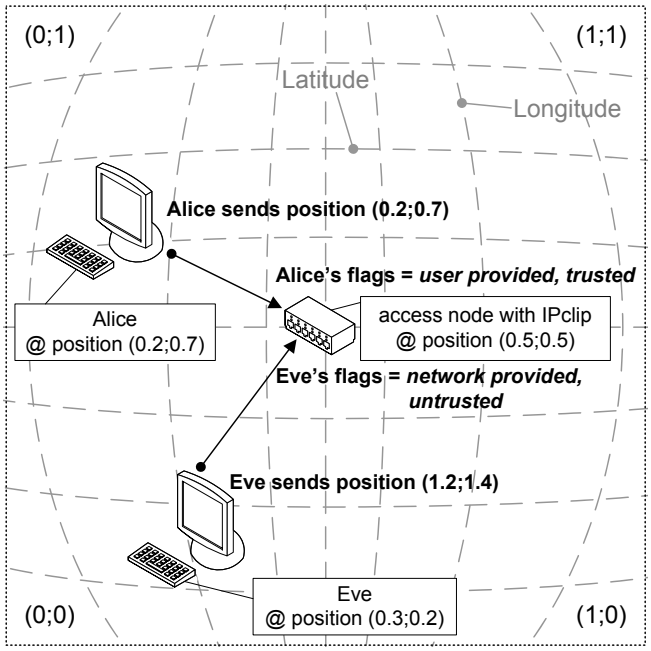

Fig. 5. Verification of the location information

node's own position as drawn in Figure 5. Values in brackets denote positions whereas grey dashed lines mark longitude and latitude. The edge length of the square (in meters) is configurable and defined as the geometric dimension of the SCA of the respective AN. In Figure 5, the edge length and the hosts' positions have been normalized to one to simplify matters. In a realistic scenario, they are given in GPS coordinates. The AN is located at the square's center (0.5;0.5). If user provided LI matches any point within the square, the IPclip flags are set to `user provided/trusted` (see Table 3). This is the case for Alice, who sends her true position (0.2;0.7). In case of an incorrect user provided LI—misconfigured, mistakenly or intentionally—IPclip can either replace the existing LI with the AN's own LI labelled as `network provided/untrusted` or forward the existing LI labelled as `user provided/untrusted`. Eve, a mobile VoIP user for example, is located at position (0.3;0.2) but pretends to be at (1.2;1.4).

2.4. MTU Adaptation

By adding LI, the size of IP packets may exceed the allowed MTU of the respective communication path. Especially high volume data streams do exploit the maximum payload size. Thus, the allowed MTU is likely to be exceeded when adding extra information in the magnitude of 15 or more bytes. In this case, the packet has to be either fragmented or discarded. But fragmentation should be avoided! Signaling and retransmission are costly and deteriorate performance [10]. This is of relatively little importance on an end-host because time and memory resources usually do suffice. However, reassembling fragments within routers is inefficient because routers are primarily intended to forward incoming packets. They are not intended to hold on to packets. Furthermore, routers write

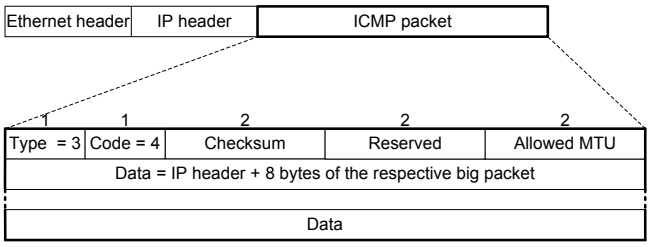

Fig. 6. Composition of an ICMP packet for PMTUD

fragments into their biggest buffers because it is not known how big the complete packet might become until the last fragment is received. Finally, with only one missing or erroneous fragment, the complete IP packet has to be retransmitted.

The reliance of IPclip on, e.g., MTU adaptation can make the system vulnerable to failures of the respective MTU adaptation mechanisms. To reduce this reliance, a possible solution is to use a smaller IP MTU by default for critical services, which guarantees fragmentation-free transport within the carrier network.

However, IPclip must support MTU adaptation. Thereby, the point when the MTU is negotiated as well as the mechanism for the negotiation depends on the characteristics and specification of the access network. Designated transport mechanisms in DSL-based access networks are IPoE and PPPoE [11]. For IPclip, both transport mechanisms are examined below.

2.4.1. IPoE

For IPoE, the MTU adaptation is done whenever a packet is received that exceeds the maximum MTU. The so-called Path MTU Discovery (PMTUD) is used for dynamic adaptation to the smallest MTU in the data path [12]. If PMTUD is supported by a host, the Don't Fragment (DF) bit of the IP header is set. That is, no fragmentation of packets exceeding the MTU shall take place. If a packet needs to be dropped due to MTU violation, an Internet Control Message Protocol (ICMP) message is sent to the packet's origin. This ICMP message passes information about the size of the allowed MTU to the sending host, which sends subsequent packets with appropriate payload size.

Figure 6 shows the structure of an ICMP message for PMTUD. ICMP is encapsulated in IP and has a 4-byte header and an optional data field [12]. An ICMP message is generated if a packet including the new IP option would exceed the allowed MTU. Thus, only packets complying with the path MTU after insertion of the IP option are forwarded.

2.4.2. PPPoE

A PPPoE connection is negotiated between two communicating entities [13, 14]. The flow of the PPPoE protocol falls into three phases: discovery phase, session phase, and termination. During the session phase, the MTU is negotiated as part of the link establishment using Link Control Protocol (LCP)

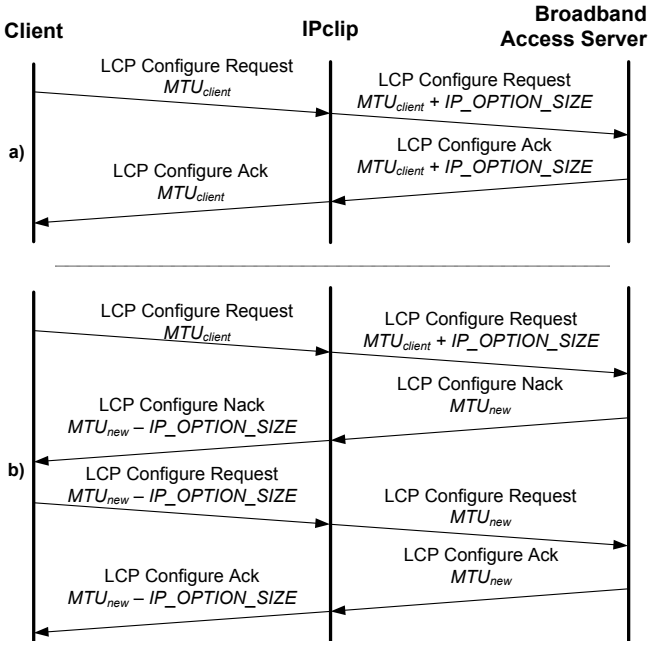

Fig. 7. Sequence of control messages with interposed IPclip mechanism if a) the Broadband Access Server agrees or b) does not aggree

Configure packets. Here, IPclip intervenes by changing the size of the MTU in the respective LCP packets. As part of the LCP header, the code field defines a Request (0x01), an Acknowledge (0x02), or a Not Acknowledge (0x03). With the type set to 0x01, an LCP Configure Request indicates MTU negotiation. In these packets, the MTU value has to be changed.

Figure 7 exemplarily depicts the signaling between a client and an ISP's broadband access server (BRAS) with interposed IPclip functionality. A client sends a Configure Request, which proposes a certain MTU (MTU_{client}). IPclip increases MTU_{client} by IP_OPTION_SIZE. The BRAS receives the Request with $MTU_{client} + IP\_OPTION\_SIZE$ and responds with a Configure Acknowledge, which contains the confirmed value. IPclip scales this value to MTU_{client} and forwarded it to the client (Figure 7a). Now, the client will use MTU_{client} when sending packets.

If the BRAS does not agree to MTU_{client}, it sends a Configure Not Acknowledge together with an own proposal (MTU_{new}). This value has to be modified to $MTU_{new} - IP\_OPTION\_SIZE$ by IPclip. Having received the Configure Not Acknowledge, the client sends a Configure Request containing $MTU_{new} - IP\_OPTION\_SIZE$. IPclip updates this value to MTU_{new}, which the BRAS receives and acknowledges (Figure 7b). As a result, the client will send packets with an MTU of $MTU_{new} - IP\_OPTION\_SIZE$.

2.5. Requirements and Constraints

To guarantee Trust-by-Wire and correct operation of IPclip as well as to consolidate the use case discussed in Section 4, some constraints need to be taken into account.

1. The existence of an IPclip-capable IP stack is necessary in those network elements and end-hosts, which make use of IPclip options. In other network elements, standard-compliant IP options must at least be recognized and skipped.

2. A fully IPclip-terminated domain is mandatory. Already a single AN without any IPclip functionality opens risky loopholes in the network infrastructure—especially when using IPclip in security applications. IP packets with manipulated LI and even fiddled flags can be injected into the network without being validated by a trustworthy IPclip instance. Thus, the presence of IPclip at all access nodes is obligatory. A practicable IPclip domain, for example, would be a single self-contained provider network.

3. Legal questions on the availability, the analysis, and the storage of sensitive, private information do arise since IPclip envisages the addition of LI to every IP packet. But generally, these questions are out of the scope of this paper. Moreover, these questions are the same as are already discussed in other areas dealing with similarly private information. Reference [5] even encourages the industry to find a solution "*even though privacy issues are taken into account*".

Put in a nutshell, the main tasks of the IPclip mechanism are:

1. Add LI in form of IP options to IP packets.
2. Identify and validate existing, user provided LI.
3. Adapt the MTU of the respective communication path.
4. (Optionally) Replace user provided LI from IP packets when LI does not pass verification.
5. (Optionally) Remove LI from IP packets in downstream data path.

3. STATE-OF-THE-ART IN VOIP EMERGENCY CALLS

A recent draft summarizes the best current practice for VoIP ECs [5]. Various regional workarounds exist, which mainly base on additional push/pull approaches, data base lookups, and manual updates of LI. There are also service providers, which do not yet support emergency services for VoIP.

The Session Initialization Protocol (SIP) is prevalently used for VoIP connection establishment. Currently, a user is required to update his location in case of changes by sending updates to his VoIP provider. In case of an EC, the user retrieves his LI via the Dynamic Host Configuration Protocol (DHCP) [15]. Those configuration servers shall also contain a SIP registrar where the host can register within the local domain. Therefore, DHCP offers the possibility to convey LI in the form of civic addresses or geospatial location attributes [9, 16]. LI may also be delivered by external information systems, e.g., Location Information Server (LIS) [17]. Location-to-Service Translation (LoST) servers map the LI of the host to the Uniform Resource Identifier (URI) of the responsible PSAP to establish the connection to the PSAP [18]. These frameworks are detailed in [4, 18]. A similar scheme is illustrated in [5].

Nevertheless, emergency services cannot be accessed in nomadic VoIP environments with varying LI unless the user manually updates his position [3, 19]. Alternatively, he could enter his location directly during an EC. Both possibilities are onerous tasks. Moreover, ECs are usually not made without reason—due to an accident, a user might not be able to enter his location by himself.

4. USE CASE – VOIP EMERGENCY CALLS

In contrast to the best current practices, the Trust-by-Wire framework approaches the problem from a different perspective. IPclip takes on the insertion of LI by either the CPEs or the ANs as shown in Figure 8. This completely replaces push/pull approaches or other mechanism as mentioned in Section 3. The user is not requested to constantly update his LI or to insert it himself. IPclip options can thereby be added into every IP packet or only into selected packets, e.g., into every SIP packet. Basically, there are two possible origins for the IPclip option and LI:

User provided: If the user's mobile gadgetry incorporates a GPS module or the like, the user's accurate position can automatically be transmitted as IP option in the event of an EC. The GPS coordinates can be used at the PSAP to retrieve a civic address or to pinpoint the user on a map if no civic address is available in uninhabited areas.

Network provided: The hard-coded LI of the AN, its ID, and the port number are inserted if no IPclip option exists or incorrect LI has been provided (incorrect with respect to the SCA of the AN).

Thus, trustworthy and accurate LI is always available to localize emergency callers—at least with the accuracy of the AN. However, both variants are an improvement for users of mobile IP phone services compared to the best current practice. The IPclip mechanism is furthermore compatible to current standardization approaches as reviewed in Section 3 and provides supplementary information.

5. CONCLUSION

The paper discussed an approach to guarantee Trust-by-Wire in packet-switched IPv4 networks. A new mechanism called IPclip provides the required functionality. The Trust-by-Wire approach and IPclip are thereby inspired by the CLIP function of classical ISDN telephone networks. It is now feasible to identify a physical line in IP-based packet-switched networks by using trustworthy LI. A fully functional hardware prototype is is presented in [20].

A broad range of services and security mechanisms can build upon the general IPclip functionality. In this paper, ECs in nomadic VoIP environments have exemplarily been chosen

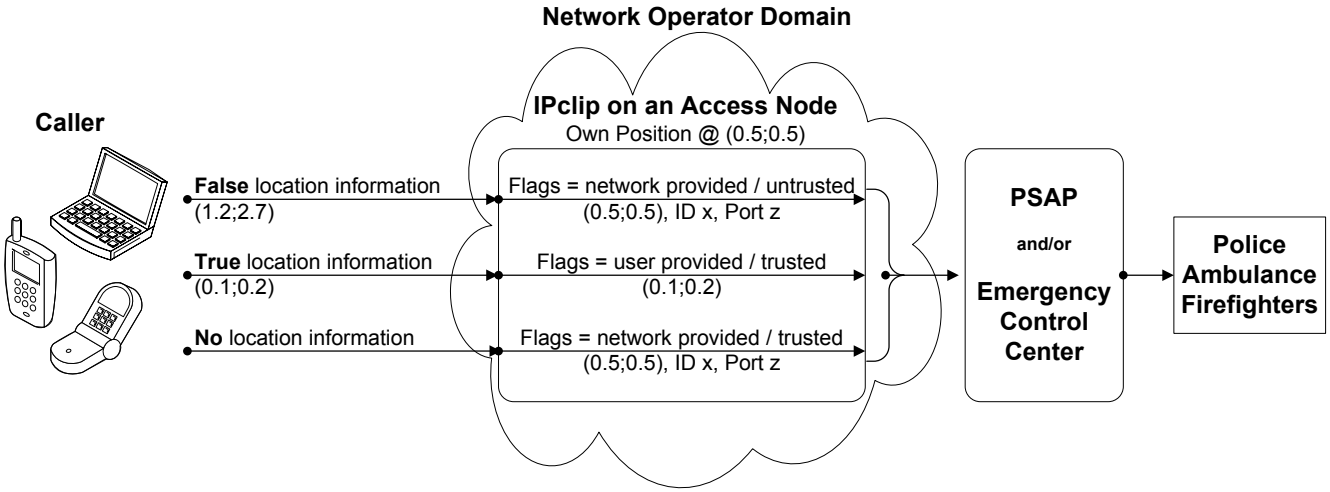

Fig. 8. VoIP ECs in an IPclip-capable environment. A caller can immediately be redirected and connected to the correct PSAP using IPclip location information. LI and flags are given with respect to the access node's SCA (compare with Figure 5)

as use case to emblematize the IPclip mechanism. The user is no longer required to update his own location. Due to the availability of trustable LI, VoIP ECs can be redirected to the correct, responsible PSAP and callers can be located reliably. A second use case addressing protection against phishing attacks is discussed in [21].

6. REFERENCES

[1] Leonard Kleinrock, "An Internet Vision: The Invisible Global Infrastructure," *Ad Hoc Networks*, vol. 1, no. 1, pp. 3–11, 2003. 1

[2] Leonard Kleinrock, "The Internet Rules of Engagement: Then and Now," *Technology in Society – Technology and Science Entering the 21st Century*, vol. 26, no. 2-3, pp. 193–207, 2004. 1

[3] Newport Networks Ltd., "Emergency Call Handling in VoIP Networks," White Paper, 2006. 1, 2, 6

[4] B. Rosen and J. Polk, "Best Current Practice for Communications Services in Support of Emergency Calling," Internet Draft, 2006. 1, 6

[5] High Level Policy Task Force on VoIP, "Common Position on VoIP (Draft)," Tech. Rep. ERG (07) 56 Rev1, European Regulators Group (ERG), 2007. 2, 6

[6] Information Sciences Institute University of Southern California, "Internet Protocol Specification," RFC 791, 1981. 2

[7] Internet Assigned Numbers Authority (IANA), "IP Option Numbers," 2007. 2

[8] National Marine Electronics Association (NMEA), "NMEA 0183 Standard," January 2002. 3

[9] J. Polk, J. Schnizlein, and M. Lisner, "Dynamic Host Configuration Protocol Option for Coordiante-based Location Configuration Information," RFC 3825, 2004. 3, 6

[10] Cisco Systems, "Resolve IP Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IPsec," White Paper, 2006. 4

[11] Juniper Networks, "Understanding PPPoE and DHCP," White Paper, 2006. 5

[12] J. Mogul and S. Deering, "Path MTU Discovery," RFC 1191, 1990. 5

[13] W. Simpson, "The Point-to-Point Protocol (PPP)," RFC 1661, 1994. 5

[14] L. Mamakos et al., "A Method for Transmitting PPP over Ethernet," RFC 2516, 1999. 5

[15] R. Droms, "Dynamic Host Configuration Protocol," RFC 2131, 1997. 6

[16] H. Schulzrinne, "Dynamic Host Configuration Protocol Option for Civic Addresses Configuration Information," RFC 4776, 2006. 6

[17] National Emergency Number Association (NENA), VoIP-Packet Technical Committee, "Interim VoIP Architecture for Enhanced 9-1-1 Services," Technical Report 08-001, Issue 1, December 2005. 6

[18] B. Rosen et al., "Framework for Emergency Calling in Internet Multimedia," Internet Draft, 2006. 6

[19] Matthew Mintz-Habib et al., "A VoIP Emergency Services Architecture and Prototype," in *14th International Conference on Computer Communications and Networks*, San Diego, CA, USA, October 2005. 6

[20] Peter Danielis, Stephan Kubisch, Harald Widiger, Jens Schulz, Daniel Duchow, Thomas Bahls, Dirk Timmermann, and Christian Lange, "Trust-by-Wire in Packet-switched IP Networks: Calling Line Identification Presentation for IP," in *Design, Automation and Test in Europe Conference and Exhibition (DATE'08), University Booth Hardware Demonstration*, Munich, Germany, March 2008. 6

[21] Stephan Kubisch, Harald Widiger, Peter Danielis, Jens Schulz, Dirk Timmermann, Daniel Duchow, and Thomas Bahls, "Countering Phishing Threats with Trust-by-Wire in Packet-switched IP Networks – A Conceptual Framework," in *Proceedings of the 22nd IEEE International Parallel and Distributed Processing Symposium (IPDPS), 4th International Workshop on Security in Systems and Networks (SSN)*, Miami, FL, USA, April 2008. 7