Lecture Notes in Computer Science

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison
    
    Lancaster University, UK

Takeo Kanade
    Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler
    University of Surrey, Guildford, UK

Jon M. Kleinberg
    Cornell University, Ithaca, NY, USA

Alfred Kobsa
    University of California, Irvine, CA, USA

Friedemann Mattern
    ETH Zurich, Switzerland

John C. Mitchell
    Stanford University, CA, USA

Moni Naor
    Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
    University of Bern, Switzerland

C. Pandu Rangan
    Indian Institute of Technology, Madras, India

Bernhard Steffen
    TU Dortmund University, Germany

Madhu Sudan
    Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos
    University of California, Los Angeles, CA, USA

Doug Tygar
    University of California, Berkeley, CA, USA

Gerhard Weikum
    Max Planck Institute for Informatics, Saarbruecken, Germany
Tai-hoon Kim  Young-hoon Lee
Byeong-Ho Kang  Dominik Ślęzak (Eds.)

Future Generation
Information Technology

Second International Conference, FGIT 2010
Jeju Island, Korea, December 13-15, 2010
Proceedings

Springer
Preface

As information technology (IT) becomes specialized and fragmented, it is easy to lose sight that many topics have common threads and because of this, advances in one sub-discipline may transmit to another. The presentation of results between different sub-disciplines encourages this interchange for the advancement of IT as a whole.

This volume comprises the selection of papers presented at the Second International Mega-Conference on Future Generation Information Technology (FGIT 2010), composed of the following 11 international conferences: Advanced Software Engineering and Its Applications (ASEA 2010), Bio-Science and Bio-Technology (BSBT 2010), Control and Automation (CA 2010), Disaster Recovery and Business Continuity (DRBC 2010), Database Theory and Application (DTA 2010), Future Generation Communication and Networking (FGCN 2010), Grid and Distributed Computing (GDC 2010), Multimedia, Computer Graphics and Broadcasting (MulGraB 2010), Security Technology (SecTech 2010), Signal Processing, Image Processing and Pattern Recognition (SIP 2010), as well as u- and e-Service, Science and Technology (UNESST 2010).

In total, 1,630 papers were submitted to FGIT 2010 from 30 countries. The submitted papers went through a rigorous reviewing process and 395 papers were accepted. Of these 395 papers, 60 were assigned to this volume. In addition, this volume contains 7 invited papers and abstracts. Of the remaining accepted papers, 269 were distributed among 8 volumes of proceedings published by Springer in the CCIS series. 66 papers were withdrawn due to technical reasons.

We would like to acknowledge the great effort of all in the International Advisory Boards and International Program Committees, as well as the organizations and individuals who supported the idea of publishing this volume, including SERSC and Springer. Also, the success of FGIT 2010 would not have been possible without the huge support from our sponsors and the work of the Chairs and Organizing Committee.

We are grateful to the following keynote speakers who kindly accepted our invitation: Hojjat Adeli (Ohio State University), Ruay-Shiuang Chang (National Dong Hwa University), and Andrzej Skowron (University of Warsaw). We would also like to thank all plenary and tutorial speakers for their valuable contributions.

We would like to express our greatest gratitude to the authors and reviewers of all paper submissions, as well as to all attendees, for their input and participation.

Last but not least, we give special thanks to Rosslin John Robles and Maricel Balitanas. These graduate school students of Hannam University contributed to the editing process of this volume with great passion.

December 2010

Tai-hoon Kim
Young-hoon Lee
Byeong-Ho Kang
Dominik Ślężak
Security, Software Engineering, Communication and Networking

Enhanced Technique for Secure Wireless Sensor Routing with Respect to Energy Conservation ........................................ 376
Maqsood Mahmud, Abdulrahman Abdulkarim Mirza, Ihsan Ullah, Naveed Khan, Abdul Hanan Bin Abdullah, and Mohammad Yazid Bin Idris

End-to-End Security Methods for UDT Data Transmissions ........ 383
Danilo Valeros Bernardo and Doan B. Hoang

Evading Virus Detection Using Code Obfuscation ..................... 394
Khurram Murad, Syed Noor-ul-Hassan Shirazi, Yousaf Bin Zikria, and Nassar Ikram

High Flexible Sanitizing Signature Scheme Based on Bilinear Maps ...... 402
Wen-Chung Kuo, Jjin-Chiou Cheng, Yen-Hung Lin, and Lih-Chyau Wu

An Access Control Framework of Federated IPTV Providers for Mobile IPTV Services .......................................................... 413
María Elizabeth Aldana Díaz and Eui-Nam Huh

A Novel Scheme for PMIPv6 Based Wireless Sensor Network .......... 429
Md. Motaharul Islam, Sang-Ho Na, Seung-Jin Lee, and Eui-Nam Huh

Mobile Partial Identity Management: The Non-repudiable Minimal Mobile Identity Model ...................................................... 439
Mohammad Hasan Samadani and Mehdi Shajari

A Privacy Preserving Service Broker Architecture for Data Sharing ...... 450
Fahed Al-Neyadi and Jemal Abawajy

Checking the Paths to Identify Mutant Application on Embedded Systems ............................................................... 459
Ahmadou Al Khary Séré, Julien Iguchi-Cartigny, and Jean-Louis Lanet

Enhanced Sinkhole System by Improving Post-processing Mechanism ... 469
Haeng-Gon Lee, Sang-Soo Choi, Youn-Su Lee, and Hark-Soo Park

A Practical Methodology and Framework for Comprehensive Incident Handling Focused on Bot Response ................................. 481
Sang-Soo Choi, Myung-Jin Chun, Youn-Su Lee, and Hyeak-Ro Lee

Real Time Watermarking and Encryption Method for DMB Contents Protection ............................................................... 493
Won-Hee Kim and Jong-Nam Kim
A Novel Scheme for PMIPv6 Based Wireless Sensor Network

Md. Motaharul Islam, Sang-Ho Na, Seung-Jin Lee, and Eui-Nam Huh
Department of Computer Engineering, Kyung Hee University (Global Campus)
Youngin, Gyeonggi-do, South Korea
{motahar,davidlee}@icns.khu.ac.kr, {shna,johnhuh}@khu.ac.kr

Abstract. IP based Wireless Sensor Network (IP-WSN) is gaining tremendous importance because of its broad range of commercial applications in health care, building & home automation, asset management, environmental monitoring, security & safety and industrial automation. A network-based mobility management protocol called Proxy Mobile IPv6 has been standardized by the IETF NETLMM working group, and is starting to pay close attention among the telecommunication and Internet communities. Since host based IP mobility protocol is not feasible for the low power and low cost sensor node, network based mobility management protocol will be well suited for IP-WSN. In this paper we propose SPMIPv6 architecture, respective message formats and analyze the signaling cost and finally evaluate its performance. The result shows that the SPMIPv6 has lower signaling cost and packet delivery cost and it can improve the handover performance of UDP and TCP than the other mobility management protocol.

Keywords: NETLMM, IP-WSN, IETF, 6LoWPAN, IEEE 802.15.4.

1 Introduction

Wireless Sensor Network is comprised of a large number of sensor nodes that are densely deployed either inside the phenomenon or very close to it [1]. Advancement in the field of Wireless sensor network has enabled the development of low cost, low power, multifunctional sensor nodes that are small in size and communicate in short distances. Recently the tiny sensor nodes consisting of sensing, data processing and communicating components are capable of holding IP stack [1, 2]. That is why application of wireless sensor networks are now quite broad than the earlier. IP-WSN concept is being implemented in many sophisticated application from building and home automation to industrial manufacturing. By the introduction of adaptation layer over IEEE 802.15.4 Physical and Medium Access Control layer it becomes feasible to transmit IPv6 packet in IP-WSN [2]. Adaptation layer make usage of stateless compression technique to elide adaptation, network and transport layer header fields-compressing all the three layers down to a few bytes [3]. However IP-WSN introduces excessive signaling overhead due to its numerous tunneling over the air.
Excessive signaling cost becomes a barrier for the real life implementation of low power IP-WSN.

PMIPv6, a network based localized mobility management protocol provides mobility support to any IPv6 host within a restricted and topologically localized portion of the network and without requiring the host to participate in any mobility related signaling [5]. In this paper we have introduced the concept of PMIPv6 by modifying the functionality of its Mobile Access Gateway and Local Mobility Anchor to IP-WSN enabled gateway and anchor point. Then we propose the protocol architecture named SPMIPv6, its functional architecture, necessary message formats. Moreover we compare our network mobility model with 2D Random walk mobility model and finally evaluate performance of our proposed scheme.

The rest of the paper is organized as follows. Section 2 reviews the background related to PMIPv6 and 6LoWPAN. Proposed Sensor PMIPv6 Protocol architecture, sequence diagram of message flow, message formats and operational architecture are depicted in section 3. Section 4 shows performance evaluation by using an analytical model and mathematical analysis. Section 5 shows the simulation result. Finally section 6 concludes this paper.

2 Background

2.1 Overview of PMIPv6

The foundation of PMIPv6 is based on MIPv6 in the sense that it extends MIPv6 signaling and reuses many concepts such as the Home Agent (HA) functionality. However, PMIPv6 is designed to provide network-based mobility management support to a Mobile Node (MN) in a topologically localized domain. Therefore, an MN is exempt from participation in any mobility-related signaling, and the proxy mobility agent in the serving network performs mobility-related signaling on behalf of the MN. Once an MN enters its PMIPv6 domain and performs access authentication, the serving network ensures that the MN is always on its home network and can obtain its Home Address (HoA) on any access network. That is, the serving network assigns a unique home network prefix to each MN, and conceptually this prefix always follows the MN wherever it moves within a PMIPv6 domain. From the perspective of the MN, the entire PMIPv6 domain appears as its home network. Accordingly, it is not justifiable to configure the Care of Address (CoA) at the MN. The new principal functional entities of PMIPv6 are the mobile access gateway (MAG) and local mobility anchor (LMA). The MAG acts like an access router and LMA act as the mobility anchor point of the PMIPv6 domain.

2.2 6LoWPAN

6LoWPAN of IETF defines an adaptation layer for sending IPv6 packets over IEEE 802.15.4. The goal of 6LoWPAN is to reduce the size of IPv6 packets to make them fit in 127 bytes 802.15.4 frames. 6LoWPAN consists of a header compression scheme, fragmentation scheme and a method framing IPv6 Link Local Address on 802.15.4 network [2]. Also, it enhances the scalability and mobility of sensor networks. The IPv6 network defines the maximum transmission unit (MTU) as 1,280
bytes, whereas the IEEE 802.15.4 packet size is 127 octets. Therefore, the adaptation layer is defined between the IP layer and the MAC layer to transport IPv6 packets over IEEE 802.15.4 links. The adaptation layer is responsible for fragmentation, reassembly, header compression, decompression, mesh routing, and addressing for packet delivery under mesh topology. The 6LoWPAN protocol supports the scheme to compress the IPv6 header from 40 bytes to 2 bytes [8].

2.3 Problem Statement of 6LoWPAN

Devices used under 6LoWPAN are likely to be exceedingly resource constrained, and it is not desirable to enforce IP compliance directly onto the devices as is required by IP-based macro-mobility protocols; such protocols were designed to hide local mobility from networks on behalf of more powerful devices with additional resources and greater power. Continuous connectivity indicates that high signaling overhead is not appropriate for 6LoWPAN sensor nodes. In particular, if the sensor network supports mobility schemes, then excessive control signal transmission makes seamless connectivity difficult. 6LoWPAN is also unsuitable for real-time communications, making mitigation of excessive control signaling overhead an even more challenging issue. Even though the network mobility concept is suitable for 6LoWPAN mobility, as seen in the NEMO Basic Support protocol [13], the current 6LoWPAN packet format cannot support efficient mobility for a 6LoWPAN Mobile Router (MR). To support 6LoWPAN mobility, a 6LoWPAN MR needs to send a BU message and receive a BA message from its HA; however, the 6LoWPAN packet format only defines the fragmentation and mesh routing headers. These messages are clearly not sufficient to support the mobility of a 6LoWPAN MR, since a 6LoWPAN packet does not support compressed mobility headers for BU and BA messages.

3 Proposed SPMIPv6 Protocol

3.1 Overview of SPMIPv6 Protocol

Sensor Proxy Mobile IPv6 (SPMIPv6) protocol is proposed for network based localized mobility protocol for wireless sensor network. The SPMIPv6 architecture will consist of Sensor network based Localized Mobility Anchor (SLMA), Sensor network based Mobile Access Gateway (SMAG), numerous fully functioned IPv6 header stack enabled sensor node. In our proposed SPMIPv6 protocol SLMA will also incorporate the functionality of Authentication, Authorization, and Accounting (AAA); we call it Sensor Authentication, Authorization, and Accounting (SAAA) service. The main role of SLMA is to maintain the reachability to the sensor node’s address while it moves around within the SPMIPv6 domain, and the SLMA includes a binding cache entry for each recently registered sensor node. The binding cache entry maintained at the SLMA is more specific than LMA in PMIPv6 with some additional fields such as sensor node identifier, the sensor node’s home network prefix, and a flag bit indicating a sensor proxy registration. SMAG is just like an Edge Router. The main function of SMAG is to detect sensor nodes movement and initiate mobility related signaling with the sensor node’s SLMA on behalf of the sensor node. Since all the devices are sensor network based so it will be energy efficient and will follow
the other characteristics of 6LoWPAN. In this scheme we assume SMAG is device containing sufficient storage, processing power and unlimited power supply. The individual sensor node can either be a fully functional device containing complete IP header stack. And the other sensor node is reduced functional device. Depending on the situation the functionality of the nodes varies.

The functionality of SLMA and SMAG in SPMIPv6 are different in many ways but similar in nature in comparison with LMA and MAG of PMIPv6. The major difference is both SLMA and SMAG works with low power 6LoWPAN sensor nodes. But both SLMA and SMAG deal with a plenty of sensor nodes. SLMA will act as a topological anchor point of all the SMAG. Inbuilt AAA functionality of SLMA helps the SMAG and sensor node to move the SPMIPv6 domain.

### 3.2 Message Flow in SPMIPv6

Fig 2 shows the sequence diagram of the overall messages flow in SPMIPv6. Each step shown in the sequence diagram is described as follows:

Step 1: When a sensor node first attaches to a SMAG domain, the access authentication procedure is performed using sensor node identifier via the deployed access security protocols on the access network.

Step 2 and 3: After successful access authentication, the SMAG obtains the sensor node’s profile, which contains the sensor nodes ID, SLMA address, and supported address configuration mode, and so on from the policy store of SAAA service.

Step 4: Then the SMAG sends a proxy binding update (PBU) message including the MN Identifier to the sensor node’s SLMA on behalf of the sensor node.
Step 5 and 6: Once the SLMA receives the PBU message, it checks the policy store to ensure that the sender is authorized to send the PBU message. If the sender is a trusted SMAG, the SLMA accepts the PBU message.

![Sequence diagram in SPMIPv6](image)

**Fig. 2.** Sequence diagram in SPMIPv6

Step 7: Then the SLMA sends a proxy binding acknowledgment (PBA) message including the MN’s home network prefix option, and sets up a route for the sensor node’s home network prefix over the tunnel to the SMAG.

### 3.3 Proxy Binding Message Format for SPMIPv6

In the proposed proxy binding update and proxy binding acknowledgement message we have added a flag bit S. If S flag is set it indicates the SMIPv6 based operations. If S bit is not set then it will indicate other operations apart from SPMIPv6. The other flags indicate meaning as mentioned in [6][7][8][9]. The mobility options field has a great significance ensuring the mobility of the sensor nodes. Depending on the scenario the mobility options field contain the respective mobility options values and facilitate the sensor mobility.

![SPMIPv6 PBU Message Format](image)

**Fig. 3.** SPMIPv6 PBU Message Format
3.4 Architecture of the SPMIPv6

Fig 6 represents the functional architecture of SPMIPv6 which includes the functionality of SLMA, SMAG and Sensor node. It also depicts the interaction between the three entities. Since the sensor node is IP based so consists of all the layers including adaptation layer. Sensor node will be identified by 64 bits interface identifier. And it can easily generate its IPv6 address by combining interface identifier with network prefix provided by the corresponding Sensor Mobile Access Gateway. Here SMAG is full function device that support complete implementation of IPv6 protocol stack and sensor node is reduce function device that support minimum IPv6 protocol implementation.

Fig. 5. Operational Architecture of SPMIPv6
4 Performance Evaluation

To evaluate the total signaling costs, we compare our analytical model with MIPv6 and SPMIPv6.

The total signaling cost ($C_{\text{mipv6}}$) of the proposed scheme based on MIPv6:

$$C_{\text{mipv6}} = M_{\text{intra\_pan}} \cdot C_{\text{sd}} + M_{\text{inter\_pan}} \cdot (C_{\text{sd}} + C_{\text{bu}})$$

Where

$$C_{\text{sd}} = \alpha \cdot (RS + RA) \cdot D_{\text{sn-smag}}$$
$$C_{\text{bu}} = \beta \cdot (BU+BA) \cdot D_{\text{smag-slma}}$$

The total signaling cost ($C_{\text{spmipv6}}$) of the proposed scheme based on SPMIPv6:

$$C_{\text{spmipv6}} = M_{\text{intra\_pan}} \cdot C_{\text{sd}} + M_{\text{inter\_pan}} \cdot (C_{\text{sd}} + C_{\text{bu}})$$

Where

$$C_{\text{sd}} = \alpha \cdot (RS + RA) \cdot D_{\text{sn-smag}}$$
$$C_{\text{bu}} = \beta \cdot (PBU+PBA) \cdot D_{\text{smag-slma}}$$

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BU</td>
<td>Binding Update Message</td>
</tr>
<tr>
<td>BA</td>
<td>Binding Acknowledgement Message</td>
</tr>
<tr>
<td>PBU</td>
<td>Proxy Binding Update Message</td>
</tr>
</tbody>
</table>
Table 1. (continued)

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PBA</td>
<td>Proxy Binding Acknowledge Message</td>
</tr>
<tr>
<td>$D_{smag-sma}$</td>
<td>Distance between SMAG/MAG and SLMA/LMA</td>
</tr>
<tr>
<td>$D_{sn-smag}$</td>
<td>Distance between SN and SMAG/MAG</td>
</tr>
<tr>
<td>$M_{intra.pan}$</td>
<td>Intra PAN Mobility</td>
</tr>
<tr>
<td>$M_{inter.pan}$</td>
<td>Inter PAN Mobility</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>Unit transmission cost in wireless link</td>
</tr>
<tr>
<td>$\beta$</td>
<td>Unit transmission cost in wired link</td>
</tr>
<tr>
<td>RS</td>
<td>Router Solicitation Message</td>
</tr>
<tr>
<td>RA</td>
<td>Router Advertisement Message</td>
</tr>
<tr>
<td>$C_{sd}$</td>
<td>Sensor Mobility Cost</td>
</tr>
<tr>
<td>$C_{bu}$</td>
<td>Binding Update Cost</td>
</tr>
</tbody>
</table>

5 Simulation

In this section, we present the results of experiments evaluating the performance of our scheme, and compare the performance of our proposed scheme to MIPv6. First, we evaluated the performance of our proposed approach by mathematical analysis. Then, we set different signaling cost for the no of IP based sensor nodes in order to evaluate the consequences of our proposed scheme and MIPv6. Finally, we summarize the key characteristics of our proposed approach as compared to MIPv6 approach.

We have implemented the model and evaluate the parameter such as the signaling cost and mobility related cost presented in this paper. All of the experiments were conducted on a Windows machine with AMD Athlon(tm) 2.5 GHz CPU and 2 GB primary memory. The operating system was Microsoft Windows XP Professional Edition, and the programming tool was Visual C++ of Microsoft Visual Studio 2005.

The Fig 7 depicts the signaling cost with respect to the number of IP-WSN node in term of the MIPv6 and SPMIPv6. Signaling cost increases as the number of IP-WSN node increases. Our proposed scheme increases the performance linearly with the comparison to MIPv6. And the signaling cost increases more rapidly as the number of IP-WSN node increases. The signaling cost will be more apparent when the sensor network will be large and will cover a large geographic area.
6 Conclusion

Signaling cost and packet delivery for the individual tiny sensor node in IP-WSN is a big challenge to overcome. In IP-WSN, if the individual sensor node wants to communicate with the gateway router then it generates huge air traffics and it deteriorates the performance at a large scale. IETF NETLMM working group has standardized network based localized mobility management protocol called PMIPv6. In this paper we propose a network based IP-WSN scheme based on the PMIPv6 called SPMIPv6 and further develop the architecture, packet format, analyzing signaling cost and finally evaluate its performance. Analysis shows that the proposed scheme reduces the signaling cost and packet delivery cost. In this paper we only focus IP-WSN of the same vendor and protocol stack. In future we will focus on the virtualization of the sensor network consisting of multi vendor and heterogeneous protocol stack.

Acknowledgement

This work was supported by the Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government (MEST) (No. 2009-0069457) and by the MKE(Ministry of Knowledge Economy), under ITRC(Information Technology Research Center) program supervised by the IITA(Institute of Information Technology Advancement)(NIPA-2010-(C1090-1021-0003)). The corresponding author is Eui-Nam Huh.
References