國立暨南國際大學資訊工程學系

碩士論文

智慧電網下傳輸層協定效能之研究

Performance Evaluation of Transport Protocols in Smart Meter Networks

指導教授：吳坤熹博士

研究生：呂佳紋

中華民國一〇一年七月二十三日

國立暨南國際大學資訊工程學系

碩士論文

智慧電網下傳輸層協定效能之研究

Performance Evaluation of Transport Protocols in Smart Meter Networks

指導教授：吳坤熹博士

研究生：呂佳紋

中華民國一〇一年七月二十三日

國立暨南國際大學碩士論文考試審定書

資訊工程學系

研究生 呂佳紋 所提之論文

智慧電網下傳輸層協定效能之研究

Performance Evaluation of Transport Protocols in Smart Meter Networks

經本委員會審查，符合碩士學位論文標準。

學位考試委員會

[illegible] 委員兼召集人

楊峻權 委員

吳坤熹 委員

中華民國 一〇一 年 七 月 二十三 日

致謝

自己在這短短的兩年碩班生涯中成長許多，並獲得許多寶貴的機會參加國內外會議，像是 TANet 2011 年會、2011 年十一月的 IETF 大會、在紐西蘭的 ICST 2011 會議、以及在韓國的 IEEE ICACT 2012 會議。今年三月更獲得教育部的「學海飛颺」獎學金，到威靈頓的維多利亞大學當交換學生。這些寶貴的機會都是我當初進入研究所時從未想過的事情，有時午夜夢迴，不免懷疑自己是否有能力勝任這些挑戰。很感謝當初大學指導教授賴守全老師，誠摯地推薦我找吳坤熹老師作爲研究所的指導教授。在老師的帶領下除了學習到許多專業的知識和做研究的方法之外，更重要的是做人處事和認真生活的哲理。實驗室的學長姐十分照顧學弟妹，同儕之間也相處融洽；而且做研究遇到困難時，實驗室同學也都會熱心地伸出援手幫忙。我十分感謝老師、實驗室學長姐和同儕對我的包容和鼓勵，沒有他們也就無法成就現在的我。 也感謝父母和我的姊妹對我的支持和愛護，家庭一直是我強大有力後盾，讓我可以勇於追求自己的夢想。

論文名稱：智慧電網下傳輸層協定效能之研究

校院系：國立暨南國際大學科技學院資訊工程學系　　　　　　　　頁數：32

畢業時間：中華民國一〇一年七月　　　　　　　　　　　　　　學位別：碩士

研究生：呂佳紋　　　　　　　　　　　　　　　　　　　指導教授：吳坤熹博士

摘要

智慧電表在先進讀表基礎建設佔有非常重要的地位，其目標是協助電力公司和使用者更有效率地使用電力資源。智慧電表網路是一個互動式的網路，控制訊息等電量使用訊息等許多重要的資料訊息都傳輸在智慧電表網路上。目前智慧電表網路的網路協定大多採用成熟的網際網路協定，在其上爲了提供可靠傳輸服務，必須進一步搭配提供可靠傳輸服務的傳輸層協定。SCTP 是新的可靠傳輸層協定，並支援 multi-homing 和 multi-streaming 等適用於智慧電表網路的機制。藉由 SCTP，兩節點間可以建立不同路徑的多條連線；當主要網路連線有問題中斷時，SCTP 可以透過備援網路路徑繼續傳輸資料。經由 Linux 平台實作驗證的結果顯示，當封包遺失率小於 10%時，SCTP 比 TCP 有較好的吞吐量;因此智慧電網可以採用 SCTP 爲傳輸層協定，以便提供更可靠和穩定的傳輸服務。

關鍵詞：SCTP；先進讀表基礎建設；智慧電表

Title of Thesis: Performance Evaluation of Transport Protocols in Smart Meter Networks
Name of Institute: Department of Computer Science and Information Engineering, College of Science and Technology, National Chi Nan University Pages: 32
Graduation Time: July 2012 Degree Conferred: Master
Student Name: Chia-Wen Lu Advisor Name: Dr. Quincy Wu

Abstract

A smart meter is crucial in the advanced metering infrastructure (AMI), which aims to assist the provider and customers working together to utilize electrical energy more efficiently. Smart meter networks are interactive networks which transport many messages (e.g. control messages, electrical usage messages) between providers and customers. Due to the maturity of Internet Protocol (IP), it is foreseen as a popular network layer protocol for smart meter networks. However, the best-effort service model of IP requires it to work with a higher layer reliable transport protocol in order to deliver critical messages in smart meter networks. Stream Control Transmission Protocol (SCTP) is a new reliable transport protocol with multi-homing and multi-streaming mechanisms. When a primary network path breaks down, SCTP connections can still continue transmitting data via backup path, and this mechanism is transparent to upper layer applications. According to the experiments on Linux platforms, SCTP can achieve higher throughput than TCP when the packet loss rate is less than 10% . This makes SCTP a suitable protocol to provide a reliable and stable communication services in smart meter networks.

Key words: AMI; SCTP; Smart Meter

Contents

List of Figures

List of Tables

Chapter 1. Introduction

The cause of high electrical energy consumption is dominated by daily usage from many areas such as households, industries, transportation and so on. Electricity demand is not only causing electrical energy resources to be depleted at a dreadful rate but also speeding up global warming by generating considerable carbon emissions. A smart meter is an intelligent device which can measure electronically how much energy is consumed and communicate the collected data to another device. For example, smart meters can send the electricity consumption data of household devices to a server on remote networks. The server is responsible for collecting the messages from smart meter networks and analyzing the data delivered by these messages. Customers are thus able to check how much energy they consume as well as the real-time pricing of electricity. On the other hand, based on these messages the utility companies can be well informed about the status of electricity usage from each customer, and encourage customers to reduce energy usage during times of peak demand, by providing some incentives.

Smart meters are transforming the traditional metering infrastructure towards to the advanced metering infrastructure (AMI) [1][2]. Although using smart meters instead of legacy meters will increase the cost in the short term, it can mitigate the need to build new power plants as well as optimize the utilization of electricity that has been bought from expensive energy sources. Smart meter networks involve one-way or two-way communication depending on requirements of customers and providers. Meter communications can either be from a meter to other devices inside the same local area network, from the meter to the provider’s information technology (IT) infrastructure or both.

Due to the maturity of the Internet protocol (IP) makes it as a popular network layer protocol adopted in smart meter networks. There are many messages are transmitted in smart meter networks (e.g. electricity usage message, billing messages) which requirement reliable and stable transmission services. However, the fundamental service model of IP simply provides best effort service which cannot meet the requirements of smart meter networks [3]. IP must be paired with a reliable transport protocol to enhance transmission services.

The Stream Control Transmission Protocol (SCTP)[4][5][6][7] has been proposed by the Signaling Transport Working Group (IETF SIGTRAN) of the Internet Engineering Task Force in order to transport signaling messages (e.g. SS7), which have requirements for reliable and timely delivery, over IP network. The new transport layer protocol-SCTP has addressed the disadvantages of UDP and TCP and also provides new features (e.g. multi-homing, multi-streaming).

In this thesis, we proposed the adoption of SCTP as the transport layer protocol which can collaborate with IP in order to provide a reliable and scalable transmission services for smart meter networks. Besides, this thesis presented the empirical comparison between transport layer protocols-TCP and SCTP in smart meter networks and also gives some suggestions about communication protocols which can adopt in smart meter networks for smart meter network designers.

Chapter 2. Related Works

An endpoint can utilize the multi-homing feature at application layer, transport layer, network layer, or even link layer. However, rewriting an application to support multi-homing takes a tremendous effort which discourages developers from doing so. Therefore, implementing multi-homing with the underlying protocols is a more popular approach. In this chapter, a few previous works about multi-homing in multi-access networks are reviewed. In Section 2.1, we describe SCTP as the transport layer approach that can bring more throughputs, and compared with the IP-layer approach, the connection over SCTP will not break down during handovers. Furthermore, in Section 2.2, we describe the challenges of wireless sensor networks when they are applied in a smart grid network. The communication protocol requirements are further investigated, which leads to the study of Chapter 3.

2.1 SCTP as a Transport Layer Solution for Wireless Multi-access Networks

With the rapid growth of the Internet and wireless communication technologies, the requirement to access the Internet has caused the development of different types of access systems. Users are expecting to access the Internet with multiple access technologies which can provide more connectivity and better services. Integrating multiple access systems and supplying more stable and connectivity services to users are critical in communication systems. In [8], SCTP was proposed as a transport layer approach for multi-access in hopes of bringing more throughputs in multi-access environments. Through three multi-access scenarios, the evaluation of throughput has been investigated with simulations in NS (network simulator) and some Linux-kernel implementations.

2.1.1 Multi-access Scenario I: Vertical Handover

A multi-access user should be capable of roaming between heterogeneous access networks without breaking any existing connections.

A multi-homed SCTP terminal was implemented with Linux which accesses the IP networks via both WLAN and GPRS. The bandwidth of WLAN is 2Mbps and the bandwidth of GPRS is 40kbps. Comparisons were made between a scenario for the network layer handover by mobile IPv6 (with TCP as transport layer protocol), and a scenario for the transport layer handover by SCTP. The experimental topology for vertical handover is shown in Figure 1.The comparison result is shown in Figure 2.

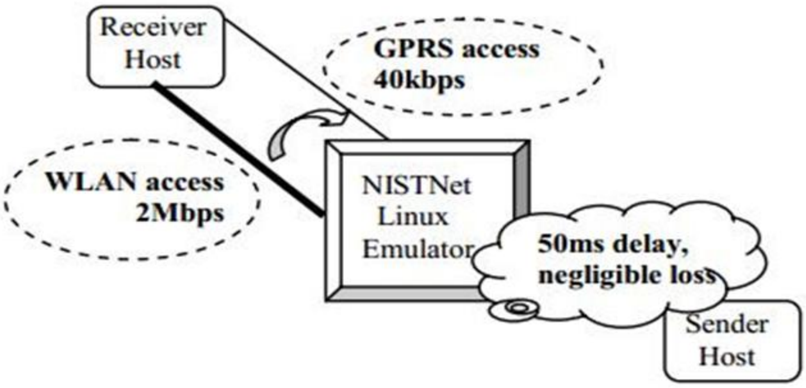

Figure 1 A vertical handover scenario

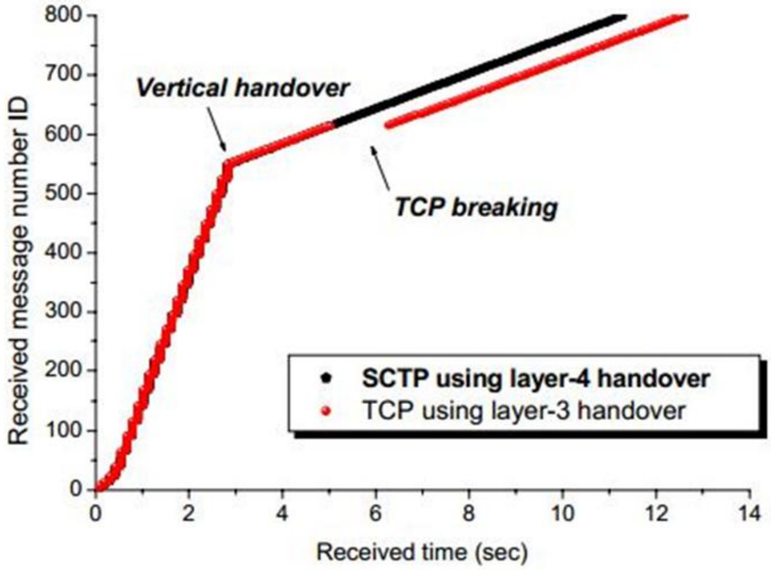

Figure 2 Vertical handover in layer4 vs layer3

In the result, we can see that the TCP connection will break down after the vertical handover from the high-bandwidth access network to the low-bandwidth access network, while the SCTP connection continues sending data smoothly.

2.1.2 Multi-access Scenario II: Alternate Retransmission

For a reliable transport protocol, when it does not receive the acknowledgement from the receiver in time, this implies that the current access network is enduring link error or congestion. It is thus better to use an alternate access network to retransmit data.

The multi-homed SCTP terminal was implemented with Linux which uses GPRS to retransmit data when the WLAN connection is interfered, collided or congested. The multi-homed SCTP over WLAN and GPRS are compared with the single-homed TCP over WLAN. The network topology for alternate retransmission scenario is shown in Figure 3.

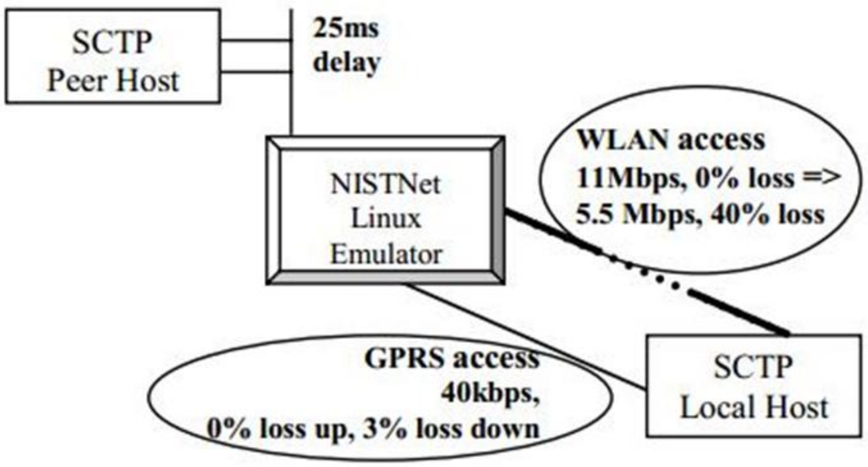

Figure 3 An alternate retransmission scenario

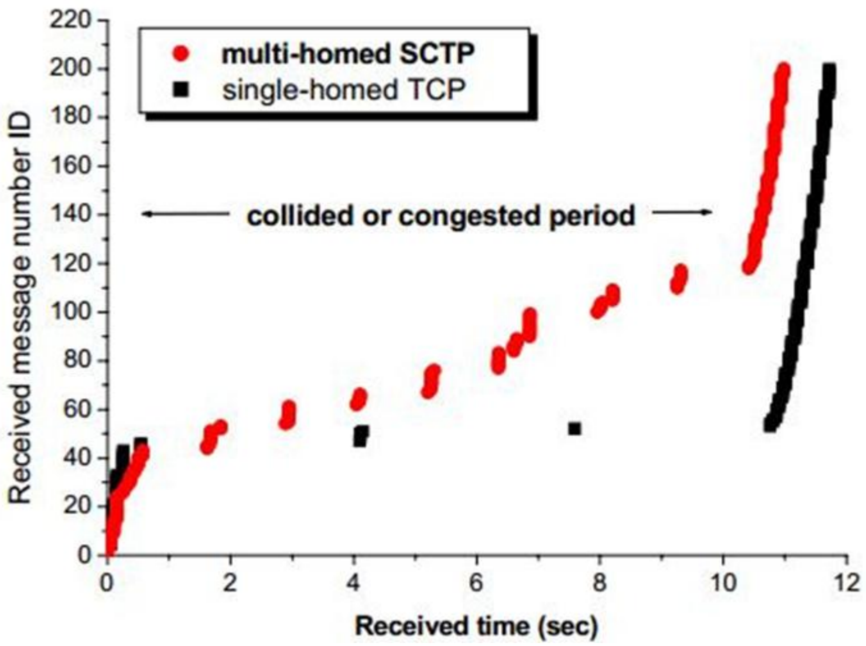

Figure 4 Alternate retransmission of SCTP vs TCP

From Figure 4 it can be clearly seen the TCP connection suffered severe losses during collided or congested period but SCTP can use the alternate path to retransmit data and recover quickly from the network accident.

2.1.3 Multi-access Scenario III: Load Sharing

In this scenario, data traffic is distributed on different flows through different available access networks simultaneously. The performance of load sharing was investigated with NS simulations to compare SCTP with IP-layer solutions..

There are four access paths between S and D and 10×100,000 bytes of data are transmitted from S to D. R1 and R2 are intermediary routers. The simulation topology is shown in Figure 5.

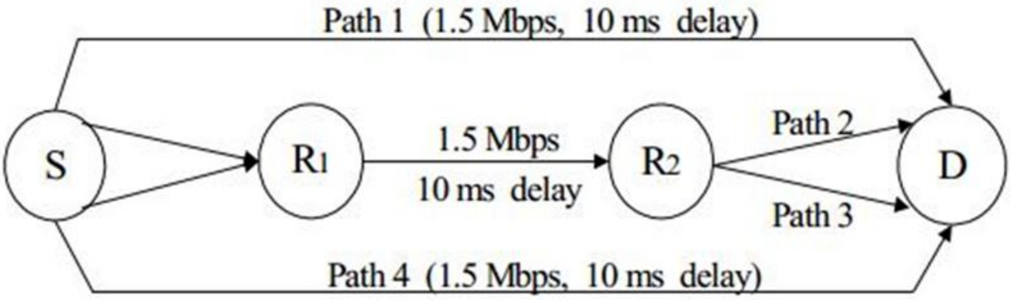

Figure 5 Simulation networks topology

Table 1 Simulation Results

Load-Sharing Scheme	Background Traffic	Link Packet Loss Rate	Transmission Time Span (s)
SCTP	No	1%	**6.926203**
IP-layer solution	No	1%	**6.835765**
SCTP	Yes	1%	**8.668651**
IP-layer solution	Yes	1%	**15.353833**

In Table 1, it can be seen that if the access paths ideally have no background traffic, the performance of SCTP is similar to IP-layer solutions. However, if the background traffic is introduced on paths, SCTP load-sharing mechanisms can achieve shorter turnaround time than IP-layer solutions.

In a word, the advantage to using SCTP as the transport layer approach is that it can avoid the network from breaking down, and it can bring more throughputs, as shown in the three key multi-access scenarios.

2.2 Opportunities and Challenges of Wireless Sensor Networks in Smart Grid

In recent years, an increasing energy demand has caused an even heavier burden on already overstressed electricity infrastructures. Furthermore, a globally increasing adaptation of renewable and alternative energy resources also introduced new issues. To address these challenges, a new generation of electricity power system, a smart grid, has emerged.

Traditional electricity power systems are typically monitored and diagnosed through wired communications. However, a cost of regular maintaining and installing communication cables are very expensive. In this respect, the collaborative and low-cost nature of wireless sensor networks (WSNs) can bring significant advantages over the traditional communication technologies used in the electricity energy systems. In [9] it was proposed that wireless automatic meter reading (WAMR) could be one of WSNs applications in a smart grid. WSNs can provide a low-cost solution that enables WAMR systems for electric utilities such as home appliances. This system provides a lot of services, such as automatic reading electricity consumption data from electric utilities and users can timely get a price of electricity via electricity management systems.

Field tests have been performed on IEEE802.15.4–compliant wireless sensor nodes (2.4-GHz frequency band) in real-world power delivery and distribution systems. In [9], the empirical measurements and experimental results provide valuable insights about IEEE802.15.4–compliant sensor network platforms and some guidelines for WSN-based smart grid applications.

In next chapter, we shall take a close look at the communication protocols and their properties that will be utilized to support a smart meter network.

Chapter 3. Communication Protocols for Smart Meter Networks

Smart meter network designers can profile a rich suite of communication protocols[10] to support smart meter networks. In this thesis, we proposed the protocols as shown in Figure 6 for smart meter networks to provide stable communication services between smart meter networks and servers on remote networks.

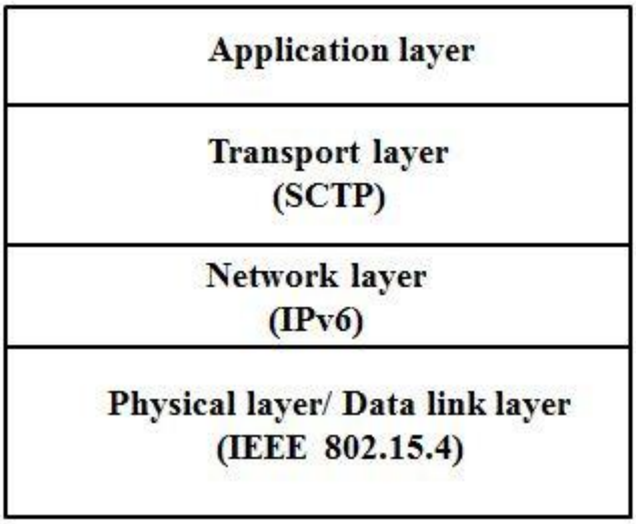

Figure 6 TCP/IP protocol suite

IEEE802.15.4[11] is a wireless communication standard protocol which was developed for wireless personal area networks (WPAN). It specifies the physical layer and data link layer in the OSI seven-layer model and focuses on low data rate, low power consumption and short distance transmission functions. The devices in smart meter networks can adopt IEEE802.15.4 as the wireless communication protocol.

Internet protocol version 6 (IPv6) supports 2^{128} IP addresses, so the numbers of addresses are more than sufficient. Even if there are a large number of devices deployed in a smart meter network, each device can be assigned with a globally unique IP address. This makes it easy for remote management. IPv6 supports stateless auto-configuration mode; a device can use EUI-64 method to derive its own IPv6 address from the MAC address of its network interface card.

Transport layer protocols are designed to provide convenient services for delivering data for the upper layer applications. In this thesis, we studied three types of transport layer protocols: user datagram protocol (UDP), transmission control protocol (TCP), stream control transmission protocol (SCTP). UDP provides unreliable service; TCP and SCTP both provide reliable services. The data from upper layer applications can choose a suitable transport layer protocol to transmit data according to the requirement of applications.

Smart meter network is a two-way service-based network which is responsible for sending electricity consumption data from home appliances while electricity providers can also send control messages to control smart meter networks through remote networks. A variety of data types such as control messages, electrical usage messages, and so forth can be transmitted between the controller server and home appliances.

Because control messages are often of critical importance, these messages need reliable transmission service, which implies that UDP is not suitable for smart meter networks. Although TCP offers a reliable service, it is still not suitable for smart meter networks due to several deficiencies of TCP such as byte-order delivery increases the risk of head of line (HOL) blocking[12]. Furthermore, it does not support multi-homing which is crucial in high-availability environments.

SCTP is a new reliable and message-oriented transport layer protocol; it not only combines the advantages of UDP and TCP but also has new powerful features unavailable in either UDP or TCP. SCTP adopts a four-way handshake sequence and a cookie mechanism to eliminate the risk of denial of service (DoS) attacks by SYN segments. Two prominent SCTP features are multi-homing and multi-streaming.

- Multi-homing[13][14]

The multi-homing feature provides a redundant mechanism between two end points, by setting up an association with multiple IP addresses or multiple network interfaces. In a smart meter network, a smart meter can control the whole local network and act as the bridge to the Internet. To take advantage of the fault-tolerant mechanism provided by multi-homing, a smart meter and a server can both have two network interfaces (as illustrated in Figure 7) bound to an SCTP association. Among the two network interfaces, one interface supports the primary network connection path and other one supports the backup path. When the primary path breaks down, SCTP will automatically switch to the backup path to continue data transmission without interruption. The failover is done by SCTP, and it is transparent to upper layer applications. This feature is very important in a high availability environment.

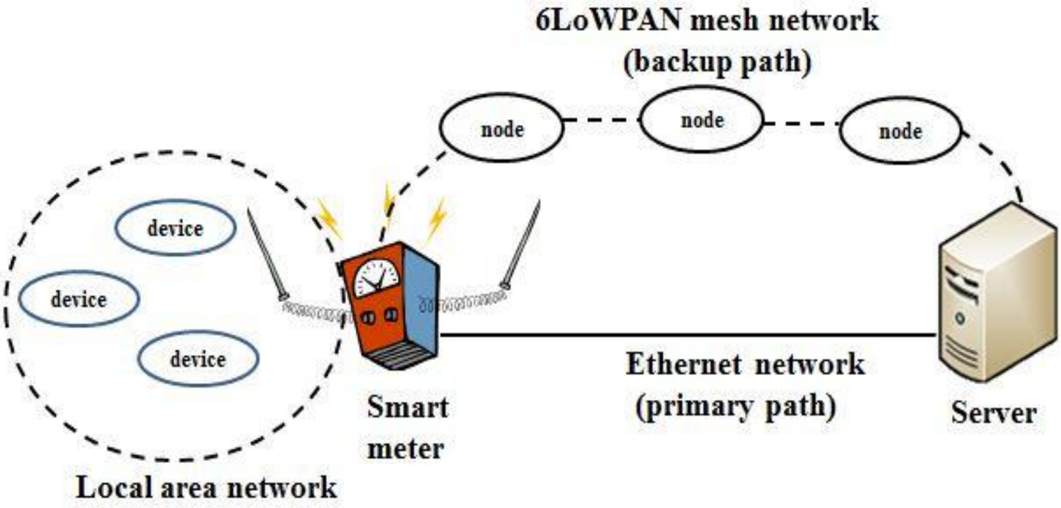

Figure 7 A smart meter network with SCTP multi-homing mechanism

- Multi-streaming[15][16]

The data from upper layer applications can be transmitted by multiple streams which are independent, as shown in Figure 8. For any stream-oriented protocols like TCP and SCTP, if a segment is lost from a specific stream, segments following the lost one will be stored in the receiver buffer until the lost one is successfully retransmitted from the sender. This situation is called Head of Line (HOL) blocking. For TCP, this implies all data transmissions must be suspended between these two end points. On the contrary, for SCTP, only one stream is blocked. Data from other streams can still be passed to/from upper layer applications. The SCTP multi-streaming feature can limit the HOL blocking effect within the scope of independent streams rather than the entire association, so that the overall performance of SCTP will not be significantly degraded.

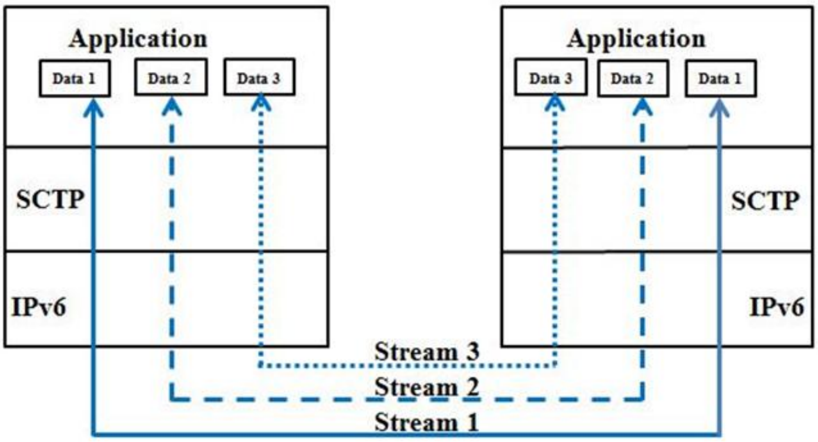

Figure 8 SCTP multi-streaming mechanism

Chapter 4. Empirical Comparison between Transport Protocols

In this thesis, evaluating the performance of TCP and SCTP on smart meter networks has been investigated in multi-homing and multi-streaming test scenarios with simulations in NS2, and also through a real implementation on Linux-kernel testing platforms[17].

In the implementation, we deployed two Linux-kernel platforms - a smart meter and a server. They are both equipped with two network interface cards, namely, an Ethernet card and a 6LoWPAN[18][19] card. The Ethernet network is a primary network connection path. When it breaks down, the connection will automatically switch to the backup 6LoWPAN network path.

6LoWPAN is designed for wireless sensor network communications which is compatible with Internet protocol version 6(IPv6). The aim of using 6LoWPAN as the backup network is that we can build a mesh 6LoWPAN wireless network between a smart meter and a server. Even the Ethernet network fails (in case the router/switch infrastructure is destroyed), it can keep transmitting data. Another advantage of using 6LoWPAN is that it does not need other overhead to perform protocol translation when the primary path resumes data transmission.

The underlying layer-2 protocol of 6LoWPAN is IEEE802.15.4. The maximum transmission unit (MTU) size of IPv6 packets is 1280 octets. However, the maximum size of an IEEE 802.15.4 physical layer packet is 127 octets. This implies that an IPv6 packet needs to be fragmented when its size is larger than 127 octets.

In other words, it makes an impact on the communication performance because it takes more overhead when the packet size is larger than 127 octets. In the following subsections, we inspect of performance of smart meter networks with two different sizes of packets; one is shorter than 127 octets (no fragmentation is required) and the other one is larger than 127 octets (the packet must be fragmented over the 6LoWPAN interface).

Section 4.1 and Section 4.2 study the communication performance of SCTP with multi-streaming and multi-homing support. More detail information and experimental results about SCTP over Ethernet/6LoWPAN are demonstrated in Section 4.3.

4.1 Simulation Results for Multi-streaming

The network simulator tool NS2[20][21] provides substantial support for simulation of transport protocols and routing protocols over wireless or wired networks. In this section, simulation of TCP and SCTP over smart meter networks is performed by the NS2 tool.

- **Network Topology**

A smart meter network topology is shown in Figure 9. S denotes a smart meter which serves as the gateway in the local network. R1 and R2 denote intermediary routers. D denotes the management server on the remote network. The simulation generates FTP data to be transmitted over the smart meter network.

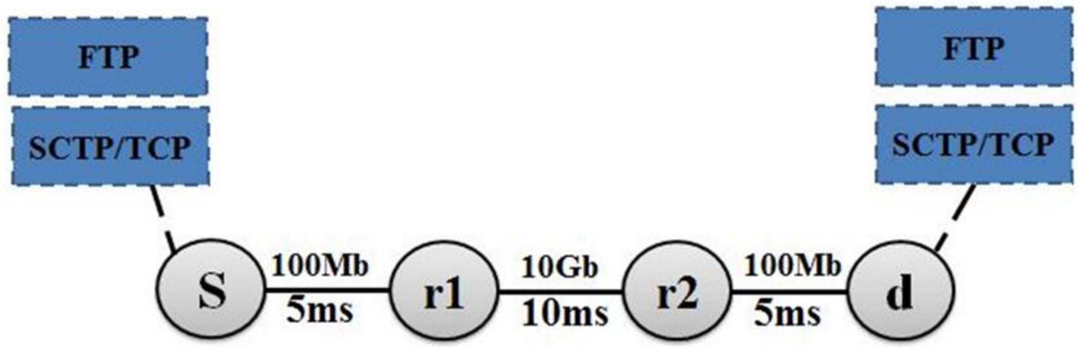

Figure 9 Network topology of the multi-streaming test scenario

- SCTP

It provides five independent streams to transmit data from the upper layer application in sequence. The size of packet is 1032 bytes when SCTP as is the underlying layer transport protocol. The 1032 bytes are composed of data chunk (1000bytes) and header (32bytes).

- TCP

It provides a single stream to transmit data from the upper layer application. The size of packet is configured to 1040 bytes when TCP is the underlying transport protocol. The 1040 bytes are composed of data (1000bytes) and header (40 bytes).

The simulation result shows that the throughput of SCTP is better than TCP when packet loss rate is less than 10% as shown in Figure 10. When the packet loss rate is greater than 10%, the performance of SCTP will decrease because almost every stream is blocked (see the HOL blocking in Chapter 3).

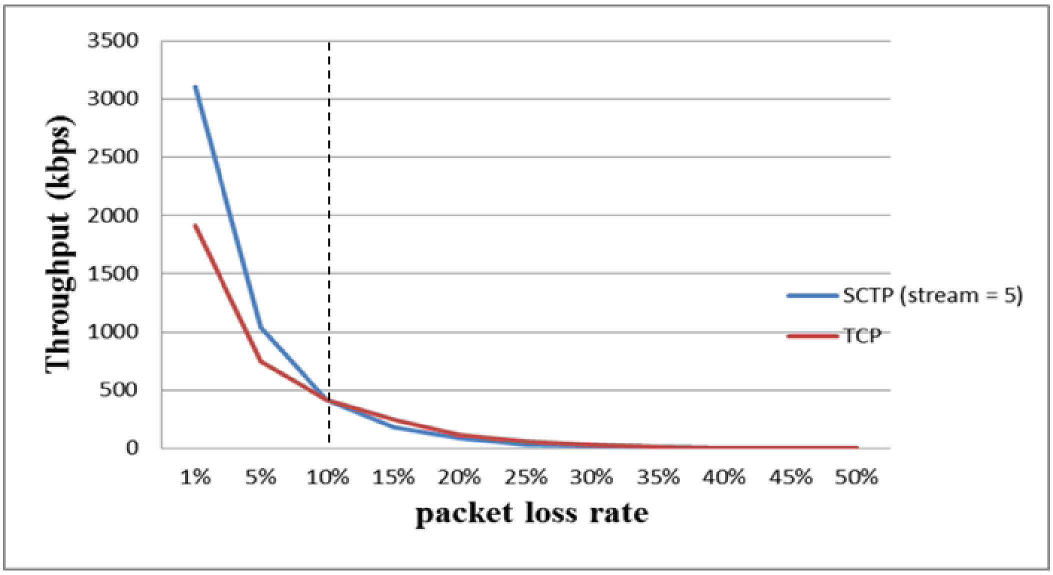

Figure 10 The throughput of SCTP and TCP (multi-streaming)

4.2 Simulation Results for Multi-homing

- **Network Topology**

As shown in Figure 11, S (smart meter) and D (server) are both equipped with two network interfaces. The primary path between S and D is s:if0 to d:if0.The backup path between S and D is s:if0 to d:if1. The simulation result is shown in Figure 12.

The total testing time is 600 seconds, S will send data from the upper ftp application to D by the primary path(s:if0-d:if0). The network interface d:if0 will be disabled at the 150th second, and enabled at the 300th second, and disabled again at the 450th second. SCTP will automatically switch to the d:if1 network interface continuing transmission data by the backup path (s:if0-d:if1).

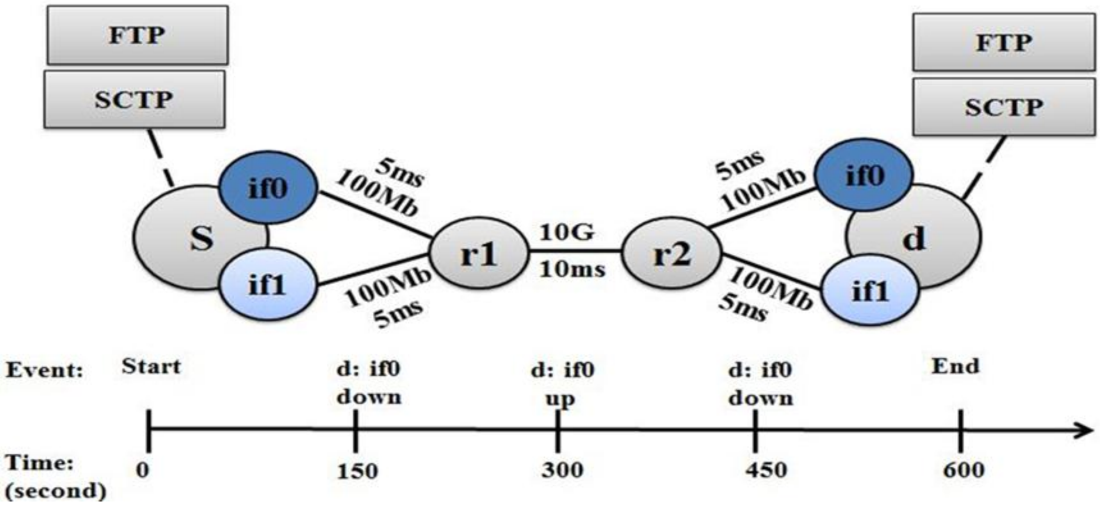

Figure 11 Network topology of the multi-homing test scenario

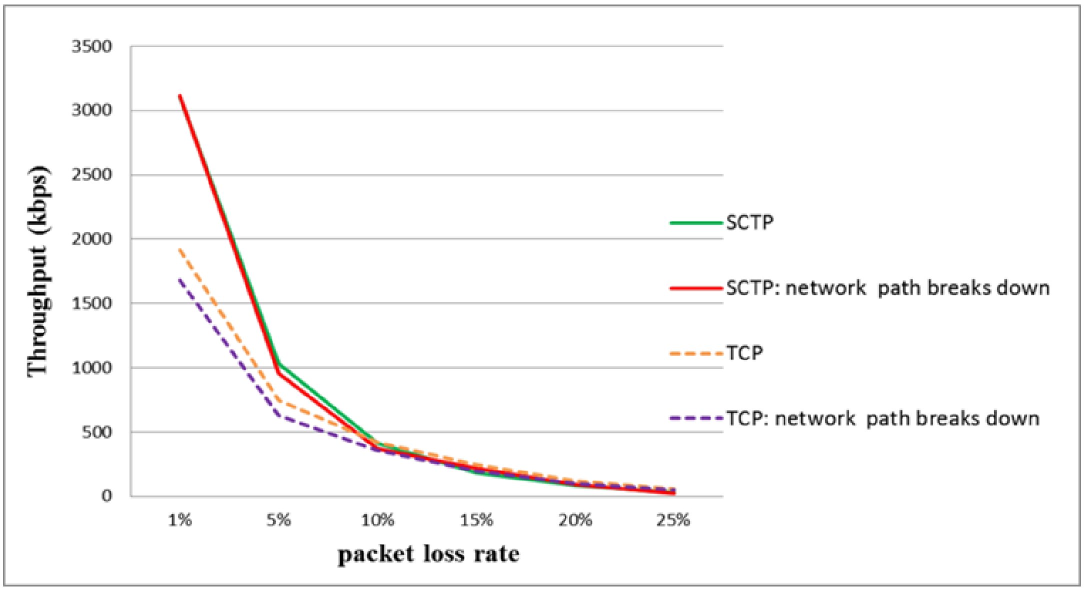

Figure 12 The throughput of SCTP and TCP (multi-homing)

There are four lines in Figure 12. The green line (A) represents the performance of SCTP without path breaking down. The red line (B) represents the performance of SCTP with path breaking down. A is very closely to B which means the performance of SCTP will be slightly affected when the network path breaks down.

The orange line (C) represents the performance of TCP without path breaking down. The purple line (D) represents the performance of TCP with path breaking down. For TCP without multi-homing mechanism, the performance degrades significantly when the network path breaks down. In Figure 13, the broken part in this figure means that the occurrence of a network path breaks down.

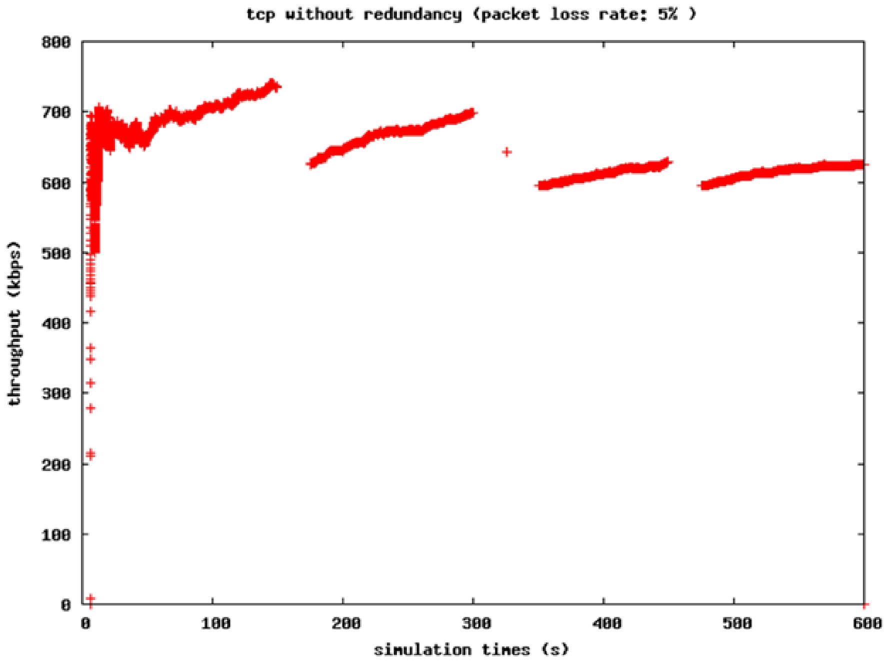

Figure 13 TCP without multi-homing mechanism support

4.3 Multi-homing on a Linux Host with Ethernet and 6LoWPAN

To verify the advantages of SCTP as shown in the above simulations, we build two Linux-kernel experimental platforms which are connected together through Ethernet and 6LoWPAN network interface cards. Ethernet network is the primary network connection and 6LoWPAN wireless network is the backup network connection.

- **System Architecture**

Figure 14 shows the system architecture in our Linux-kernel experiments. The total testing time is 500 seconds; the smart meter will continuously send data to the server by the primary path (Ethernet network) at the beginning. The Ethernet network interface of the smart meter will be disabled at the 100th second and enabled again at the 200th second. The data will be transmitted by the 6LoWPAN wireless network when the Ethernet network interface of the smart meter is disabled.

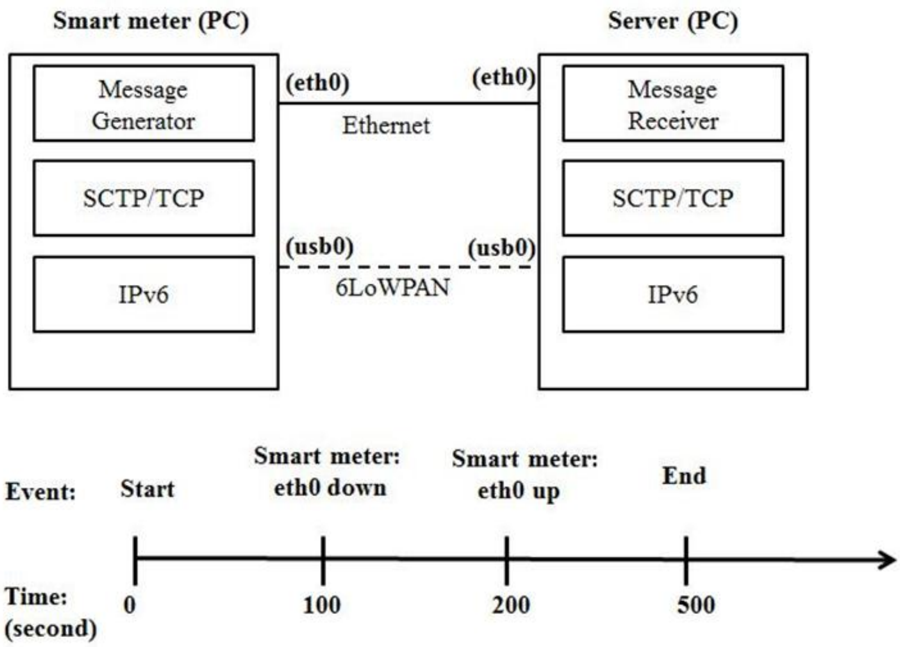

Figure 14 System architecture of the multi-homing experiments

As shown in Figure 14, there are some modules implemented on these Linux hosts:

- Message generator module

It is responsible for generating data which serve as messages transmitted in smart meter networks.

- Message receiver module

It is responsible for receiving data from the smart meter.

■ SCTP (multi-homing mechanism) /TCP module

TCP is supported by Linux in its standard library. In this work, we adopt the SCTP library provided by the Linux Kernel Stream Control Transmission Protocol (lksctp) project[22]. These libraries are used to develop C programs to implement the SCTP and TCP module.

■ IPv6 module

The smart meter and the server both have two IPv6 addresses; one is for the Ethernet network interface and the other one is for the 6LoWPAN network interface.

The parameters of the SCTP protocol parameters can also be adjusted. The following are some default parameters used in this test scenario.

- RTO.Min=1 second

  RTO-Retransmission Time-out: This value determines when to retransmit unacknowledged data.

- RTO.Max=60 seconds
- HB.interval=30 seconds

  The heartbeat (HB) will be periodically transmitted to each peer address in order to determine the reachability status of the peer's addresses.

- Path.Max.Retrans=5 attempts

  The maximum number of HB messages, it will be retransmitted to a particular destination address before making it inactive.

An SCTP packet includes SCTP header, SCTP control chunks and application data encapsulated within SCTP DATA chunks. SCTP uses transmission sequence number (TSN) to represent the sequence number in the entire data stream.

4.3.1.1 Test Scenario I

The size of application data is 41 bytes. The total size of frame is 125 bytes as shown in Figure 15. It does not require additional overhead to perform fragmentation when switching to the backup 6LoWPAN network connection path.

Frame header	**IPv6 header**	**SCTP header**	**Data**
16 bytes	40 bytes	28 bytes	41 bytes

Figure 15 The structure of packet format

- With the default of SCTP parameters (as specified in P.21):

  The failover time of SCP takes approximately 60 seconds as shown in Figure 16.

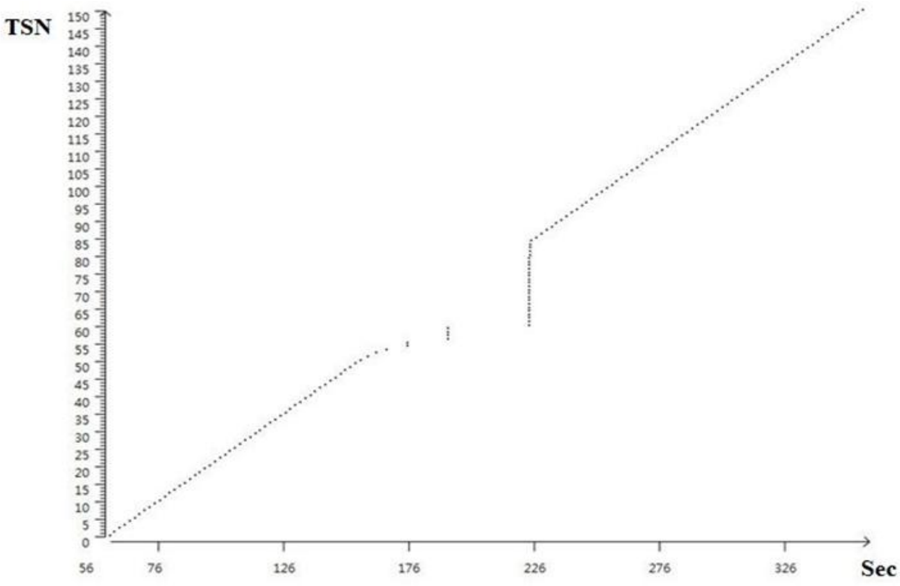

Figure 16 The TSN graph (default SCTP setting)

- However, if we adjust SCTP parameters as follows:
  - RTO.Min=200 milliseconds
  - RTO.Max=1 second
  - HB.interval=10 seconds

■ Path.Max.Retrans=2 attempts

The test result is significantly improved, as shown in Figure 17. The failover time of SCTP can be shortened by setting the relevant SCTP parameters.

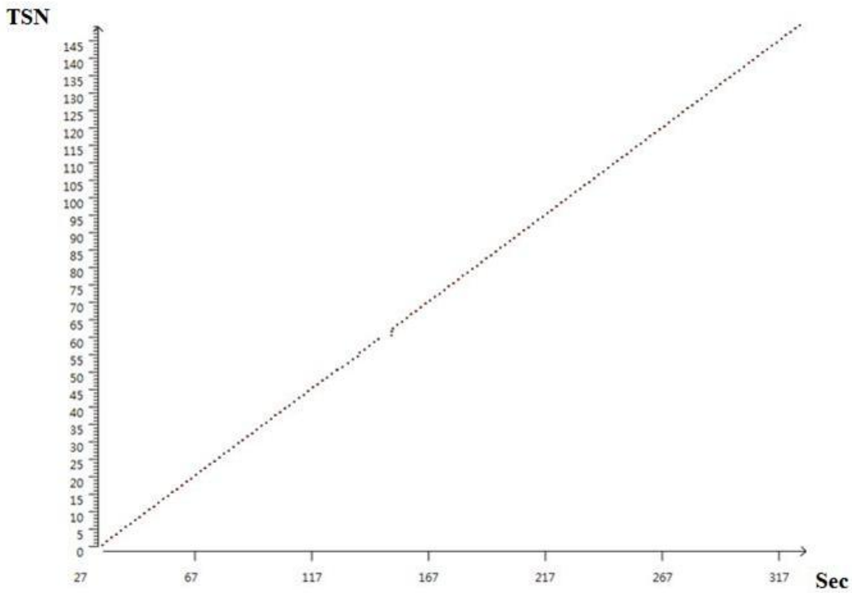

Figure 17 The TSN graph (adjustment SCTP setting)

4.3.1.2 Test Scenario II

The size of the application data is 1203 bytes. The total size of frame is 1287 bytes as shown in Figure 18; it needs fragmentation which will increase more overhead to perform packet fragmentation.

Frame header	**IPv6 header**	**SCTP header**	**Data**
16 bytes	40 bytes	28 bytes	1203 bytes

Figure 18 The structure of packet format

● With the default of SCTP parameters:

The test result is shown in Figure 19. The failover time of SCP takes approximately 120 seconds.

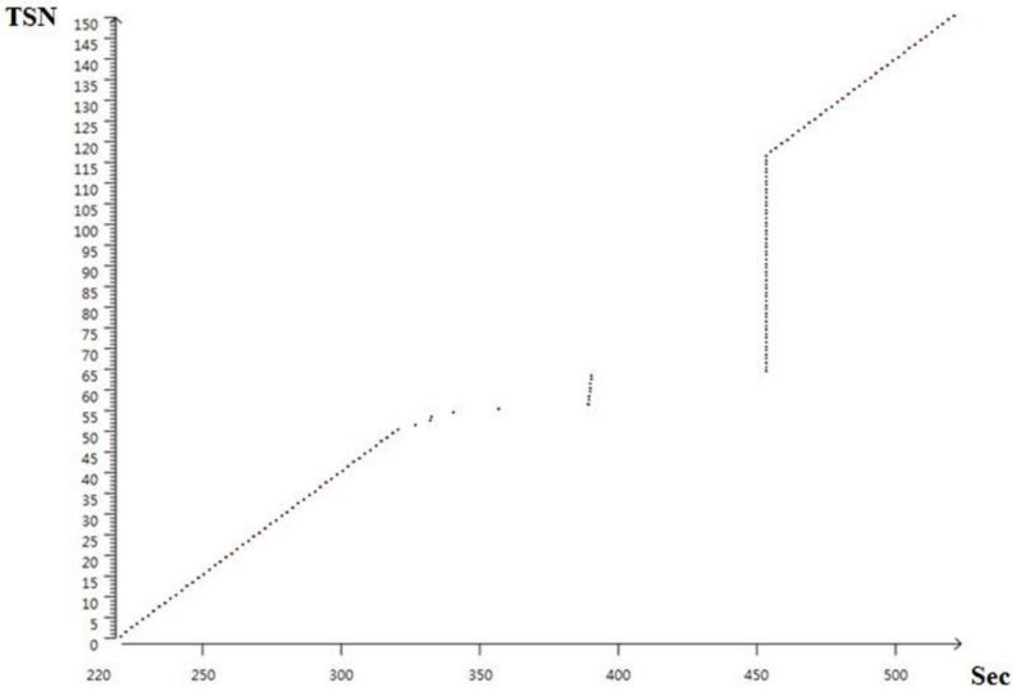

Figure 19 The TSN graph (default SCTP setting)

- With the adjusted SCTP parameters :

(These parameters are same as in Section 4.3.1.1)

- RTO.Min=200 milliseconds
- RTO.Max=1 second
- HB.interval=10 seconds
- Path.Max.Retrans=2 attempts

Compared to Figure 19, the test result is significantly improved, as shown in Figure 20. The failover time of SCTP can be shortened by setting the relevant SCTP parameters.

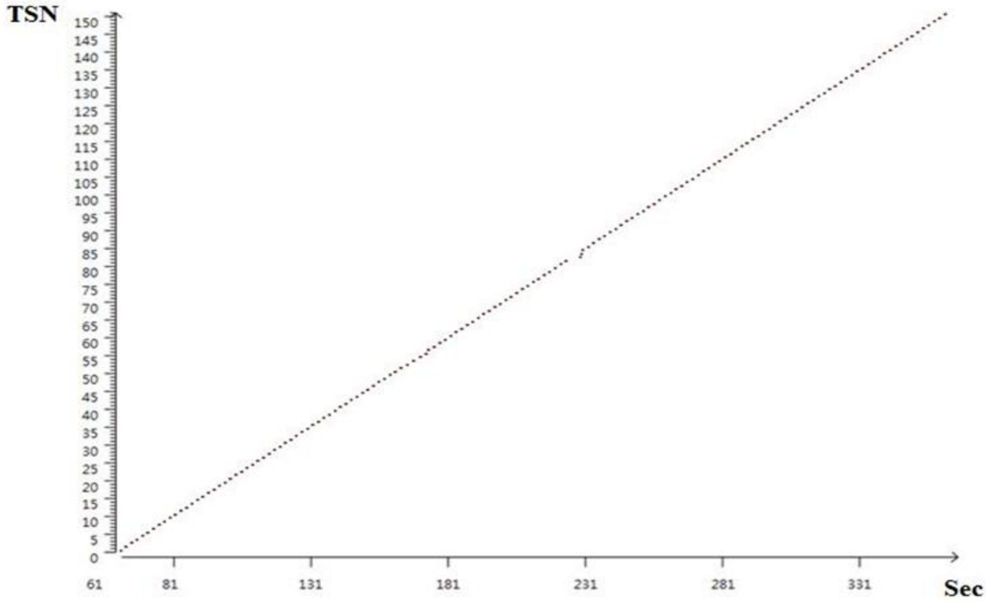

Figure 20 The TSN graph (adjustment SCTP setting)

Chapter 5. Conclusion and Future Work

In this thesis, we proposed SCTP as a transport protocol for smart meter networks. SCTP has two powerful features, namely multi-homing and multi-streaming, which can improve the reliability and efficiency of SCTP. With multi-homing mechanism, SCTP can continue transmitting data when a network interface breaks down but TCP will be forced to disconnect whenever network interfaces break down. Simulations showed that SCTP with multi-streaming mechanism can achieve higher throughput than TCP when packet loss rate is less than 10%. In an implementation with Linux, a smart meter and a server are both equipped with an Ethernet and a 6LoWPAN network interface. Furthermore, experiments showed that failover time of SCTP can be shortened by adjusting related parameters of SCTP. It can switch to the backup path (6LoWPAN) more smoothly when the primary path (Ethernet) breaks down. According to both simulations and real implementations, SCTP can provide more reliable and stable transmission services for smart meter networks.

In the future, we will further do more experiments to observe the relationship between different sizes of packets and the failover time of SCTP. Moreover, we also want to evaluate the performance of SCTP with multi-streaming support on a Linux host. Meanwhile, the security issue of smart meter networks has attracted a lot of attention in recent years. Enhanced security mechanisms to protect smart meter networks from malicious attacks and unauthorized access deserve further study.

References

[1]S. Karnouskos, O. Terzidis and P. Karnouskos, “An Advanced Metering Infrastructure for Future Energy Networks”, International Conference on New Technologies, Mobility and Security (NTMS), May 2007, Paris, France , Pages 597-606.

[2]P. Yi, A. Iwayemi, and C. Zhou , “Building Automation Networks for Smart Grids”, International Journal of Digital Multimedia Broadcasting, Volume 2011, article ID 926363, 2 April 2011.

[3]Y.-H. Jeon, “QoS requirements for the Smart Grid Communication System”, International Journal of Computer Science and Network Security, Volume 11, No 3 , March 2011.

[4]S. Fu and M. Atiquzzaman, “SCTP: state of the art in research, products, and technical challenges”, IEEE Communications Magazine, Volume 42, Issue 4, April 2004, Pages 64-76.

[5]P. Natarajan, F. Baker, P.D. Amer, and J. T. Leighton, “SCTP: What, Why, and How”, IEEE Internet Computing Magazine, Volume 13, Issue 5,Sept.-Oct. 2009,Pages 81-85.

[6]L. Caro et al., “SCTP: A Proposed Standard for Robust Internet Data Transport”, IEEE Computer Magazine, Volume 36, Issue 11, November 2003, Pages 56–63.

[7]R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. Schwarzbauer, T. Taylor, I. Rytina, M. Kalla, L. Zhang and V. Paxson,“Stream Control Transmission Protocol”,RFC2960, October 2000.

[8]Jinyang Shi, Yuehui Jin, Wei Guo, Shiduan Cheng, Hui Huang and Dajiang Zhang, "Performance Evaluation of SCTP as a Transport Layer Solution for Wireless Multi-access Networks", IEEE WCNC 2004, Pages 453-458.

[9]Vehbi C. Gungor, Bin Lu and Gerhard P. Hancke, "Opportunities and Challenges of Wireless Sensor Networks in Smart Grid", IEEE transactions on industrial electronics, Volume 57, No. 10, October 2010.

[10]F. Baker and D. Meyer, "Internet Protocols for the Smart Grid", RFC6272, June 2011.

[11] P. Baronti, P. Pillai, V.W.C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: a survey on the state of the art and the 802.15.4 and ZigBee standards", Computer Communications, Volume 30, No. 7, May 2007, Pages 1655-1695.

[12]K. Grinnemo, T. Andersson and A. Brunstrom, "Performance Benefits of Avoiding Head-Of-Line Blocking in SCTP", the Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services, October 2005.

[13]F. Siddiqui and S. Zeadally , "SCTP multihoming support for handoffs across heterogeneous networks", the Communication Networks and Services Research Conference, May 2006,Pages 8pp-250.

[14]L. Budzisz, R. Ferrus, K.-J. Grinnemo, A. Brunstrom and F. Casadevall, “An Analytical Estimation of the Failover Time in SCTP Multihoming Scenarios”, the Wireless Communications and Networking Conference, March 2007, Pages 3929 – 3934.

[15]G. Heinz, “Priorities in SCTP Multi-streaming”, Master’s Thesis, Computer and Information Sciences Dept., Univ. of Delaware, USA, May 2003.

[16]S. Samtani, J. Iyengar, and M. Fecko, “SCTP Multi-streaming: Preferential Treatment among Streams”, the Military Communications Conference (MILCOM), October 2003, Pages 966-970.

[17]G. Camarillo, R. Kantola, H. Schulzrinne, “Evaluation of transport protocols for the session initiation protocol”, IEEE Network Magazine, Volume 17 , Issue 5, Sept.-Oct. 2003,Pages40-46.

[18]N. Kushalnagar, G. Montenegro and C. Schumacher, “IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals”, RFC 4919, August 2007.

[19]G. Montenegro, N. Kushalnagar, J. Hui and D. Culler, “Transmission of IPv6 Packets over IEEE 802.15.4 Networks”, RFC4944, September 2007.

[20]Caro, J. Iyengar, “ns-2 SCTP module”, http://pel.cis.udel.edu.

[21]UC Berkeley, LBL, USC/ISI, and Xerox Parc, “ns-2 Simulator,” Version 2.29, October 2005, http://www.isi.edu/nsnam/ns.

[22]LKSCTP project, “A Linux kernel reference implementation of SCTP”, http://lksctp.sourceforge.net.