Evaluation of Energy Efficiency of Popular Mobile Payment Protocols

Munir Hussain[1], Syed Usman Jamil[2]

[1]University of Wales, Cardiff, United Kingdom.

[2]MRPP, 1 Carss Place, Charnwood 26, ACT, Australia.

munirhussain80@yahoo.com[1]

usman971@yahoo.com[2]

Abstract

Over the last few years, the popularity of both electronic and mobile commerce (M-Commerce) has increased due to advancement in the Information Technology (IT). Evaluation of E-commerce and M-commerce protocols has always remained a subject of sustained effort to find an optimal solution. Mobile devices are resource constrained in terms of memory, processing and battery power. There have been efforts in the past for evaluation of such protocols based on the issues like privacy, security and efficiency. In this paper special consideration however is given to the battery power and thus evaluates few well-known M-commerce payment protocols for their battery requirements in terms of energy cost and compares energy cost of these protocols to find the most optimal solution for mobile payment. Initial objective of this paper finds out energy consumption for every individual entity involved in the most popular mobile payments protocols. After the earlier has been achieved, the second and the most fundamental objective of this work is to calculate the overall energy consumption and to analyze these selected protocols to find out the most energy efficient protocol.

Keywords: M-Commerce, Mobile Payment Protocols, Energy Consumption.

Article Number: IOARP-JCN04-003
IOARP Journal of Communication and Networks
Volume 4, Issue 1, June 2024
Appeared on Digital Library: 15 July 2024

1. Introduction

Due to their characteristics like ease of use and simplicity, M-commerce has become one of the most-used concepts in the world today. The world of electronic transactions is switching from E-commerce to M-commerce and thus it is important to address various issues in mobile devices that may somehow relate to M-commerce. There are various issues posed to mobile devices in terms resources like memory, battery power and processing. For small handheld devices, battery is the major concern and thus it is very important to analyze the M-commerce payment protocols for their battery requirements so that the power resources may be preserved. Battery is one of the most vital resources in mobile devices thus to extend the mobile devices battery lifetime, it becomes important to save the battery resource as much as possible. With various choices of M-commerce payment protocols available, some of the payment protocols may consume less energy of mobile devices involved in the process than others. Thus, evaluation of mobile payment protocols is very important to discover the most-feasible solution.

Recent mobile technology is playing a valuable role in M-commerce field, but still it is facing a lot of issues related to hardware and operating system of mobile devices etc. M-commerce issues are not only restricted to mobile device hardware and operating system, but there are a lot of other issues than technical issues that could affect M-commerce growth. Some technical and non-technical issues are mobile device constraints, lack of standards availability issue, mobile network constraints, security issues, capability of postpone, abandon or block transaction issues, customer loyalty and technologies evolution issues [1, 2]. Today, Cell Phone, Personal Digital Assistants (PDAs), Smart Phone which is the combination PDA and Mobile Phone, Laptop and Earpiece are mostly used in M-commerce in order to complete an electronic transaction. All of these devices have very limited resources which are limited battery power, less memory and low processor speed etc. Although all of these constrained of mobile devices are vital, but the one which is more vital than other is power consumption that is why it should be kept to a minimum consumption to extend the lifetime of mobile device battery. The mobile device lifetime typically exhibits a strong dependency on battery life. The function of a mobile device regarding online payment is sending of bits across the m-commerce network to complete an electronic transaction. As during a payment transaction exchange of messages take place, so therefore, power consumption can be allocated to three functional domains: bits sending, bits processing, and bits receiving, each of which requires optimization. As loss of energy is one the most critical issues in M-commerce networks, where for the most of time mobile devices are used and its competence can be achieved by using shutting down unused/inactive components of mobile devices through operating system control, dynamic voltage and frequency scaling of the processor core ,using carefully developed processing protocols, employing energy-aware computing, controlling low-power modulation, designing adjustable and low duty cycle radio power transmission, and optimizing the energy in multi hop communication schemes techniques [3]. A more detailed and technical evaluation of the functionality of popular mobile payment protocols has already been published previously [16].

The rest of work is organized as follows: Section 2, explain the Methodology for Analysis. Section 3 gives the overview of Energy Consumption Analysis of Mobile Payment Protocols. Section 4, describe Final Results and Discussion. Section 5, makes Conclusion and finally Section 6, point out some Future Works.

2. Methodology for Analysis

The methodology section contains energy consumption during receiving and sending packets equations and gives some explanation about the generic parameters used in the energy consumption equations. Based on its content, this section is divided into two major sections. Section 2.1 is focused on explaining methodology that has been adopted to analyze various M-commerce payment protocols in this work. Section 4.2 initially describes the energy equation that is used to calculated energy cost of each protocol and notations used in the paper to follow. This section also describes parameter values and assumption in terms of parameter values.

2.1. Methodology to Analyze Protocols

Mobile devices are resource constrained in terms of memory, processing and battery power. Special consideration however is given to the battery power and this paper evaluates these M-commerce payment protocols for their battery requirements in terms of energy cost. Next section of this paper compares energy cost of these protocols to find the most optimal solution for Mobile payment. For the very purpose, four most renowned M-commerce payment protocols have been selected for evaluation. These protocols are:

- Secure Protocol for Payment System Based on Kiosk-Centric Case Mobile Scenario
- Secure Electronic Transaction (SET) Protocol
- Privacy in New Mobile Payment Protocol
- Simple Secure M-commerce Protocol (SSMCP)

The computation of energy cost for the above M-commerce protocols is divided into three main phases in terms of methodology. Phase 1 below explains the methodology for computation of energy cost per packet, Phase 2 explains the methodology to compute energy cost per entity while Phase 3 gives methodology for computation of overall energy cost for every protocol stated in bulleted points above.

2.1.1. Phase 1 (Methodology for Computation of Energy for Each Packet)

Figure 1 elaborates Phase 1 of the processing towards achieving energy cost comparison of these payment protocols. As an initial and most vital step of Phase 1 every protocol is considered in order to identify various aspects of its working. For every protocol, the whole M-commerce payment process is considered along with identification of all the packets transmitted or received during payment process by different entities involved in that protocol. It is vital to mention that to make an M-commerce transaction possible in first place, there are different entities involved in the payment process. These entities can be customer, merchant and issuer etc.

As part of Phase 1, of this paper gives a diagrammatic illustration of each payment protocol. This illustration makes it easy to identify the flow of packets between different entities and to identify the number of transmission and receptions performed by every single entity involved in the protocol. Equation 1 gives a sample packet that explains the constituents of the packet in terms of different parameters and encryption if any. Once this diagrammatic explanation is complete, it becomes very easy to identify total packets transmitted or received by all the entities during an M-commerce transaction.

$$PN_P \,||\, H\,(PN_P \,||\, PIN_P)_{PK} \tag{1}$$

Next step in Phase 1 is to calculate the size of each transmitted and received packet. Once the parameter values are known, it is a matter of simple mathematics to attain size of each transmitted or received packet however; special care is ensured while taking into account the impact is encryption on the size of a packet.

Packets are then segregated into transmissions and receptions. D. Song in [4] give energy consumption model for transmissions and receptions for mobile devices.As mobile devices are a key entity in M-commerce payment systems thus the research adopts these equations to calculate energy cost of each M-commerce payment protocol. As per Song [4] energy consumed by a mobile device for transmission of packet of size B (bytes) is:

$$E_{elec}B + E_{amp}B(d)^2 \tag{2}$$

E_{elec} in the equation above is circuit energy that is consumed in processing a packet before its transmission while E_{amp} is the amplification energy that is consumed in amplification of the packet to enable it to travel a specified distance (i.e. d). It is important to mention that both E_{elec} and E_{amp} are constants. Now as we have already calculated the size of each transmitted packet, by putting in the values of packet in the equation above would give us the energy cost of transmission of all the packets transmitted in M-commerce payment for a selected protocol.

For received packets on various entities, D. Songs [4] gives the energy equation as:

$$E_{elec}B \tag{3}$$

Here B is the size of received packet, it is understandable enough that the only energy consumed during reception would be the circuit energy. As we have already calculated the size of all the received packets in the protocol thus by putting in the value of B (i.e. size of received packet in bytes) in above equation, the energy consumed by each received packet can be calculated.

At the end of Phase 1 of this process, a list containing the energy cost of every packet transmitted or received during a transaction could be achieved. This phase is repeated for all four protocols under consideration to initially acquire all the packets transmitted and received during a transaction then calculate sizes of each packet and subsequently calculated energy cost for each packet transmitted or received.

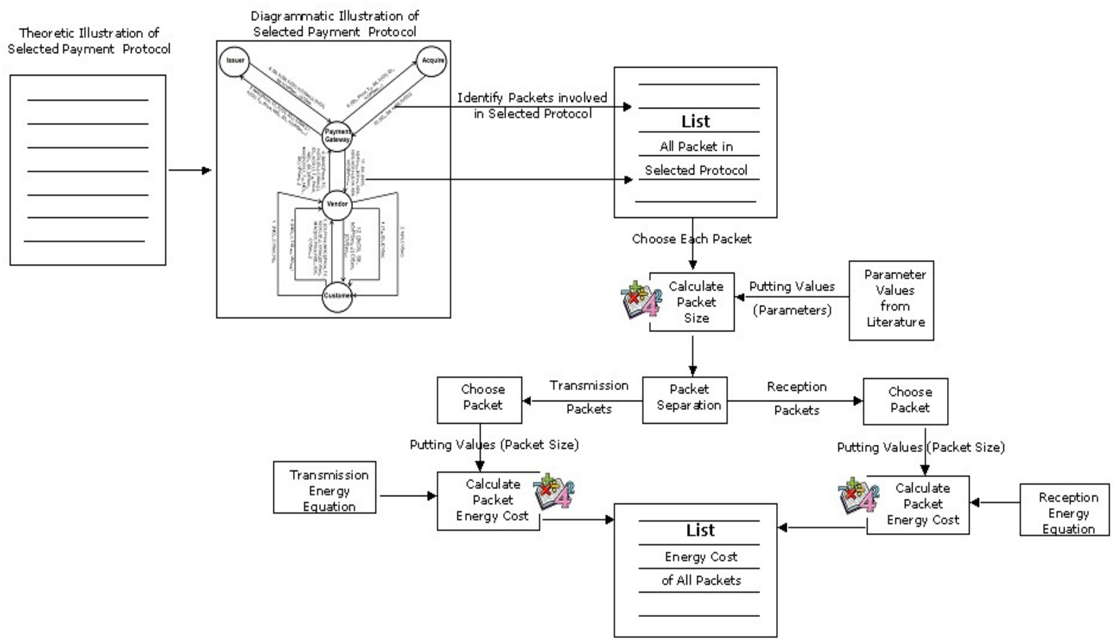

Figure 1: Methodology Architecture Phase 1

2.1.2. Phase 2 (Methodology for Computation of Energy Cost for Each Entity)

As explained above, there may be different entities involved in a protocol for M-commerce payments. In Phase 2 of the process, for every selected protocol, total number of entities participating in selected M-commerce protocol is identified. Once this is done, individual entities are selected and for each entity, the packets transmitted and received by it are identified. Phase 1 of our processing gives us a list of energy cost of all the packets for any given protocol. So for each entity, its energy cost would be a sum of the relevant energy costs of each transmitted and received packet. This process can be repeated to calculate energy consumed by all the entities for a given protocol. A list of the energy costs of all the entities could be maintained and later plotted in form of a graph for every protocol. Same is repeated for every protocol and thus energy cost of various entities in every protocol is acquired. Figure 2 attempts to elaborate further on Phase 2 of our processing.

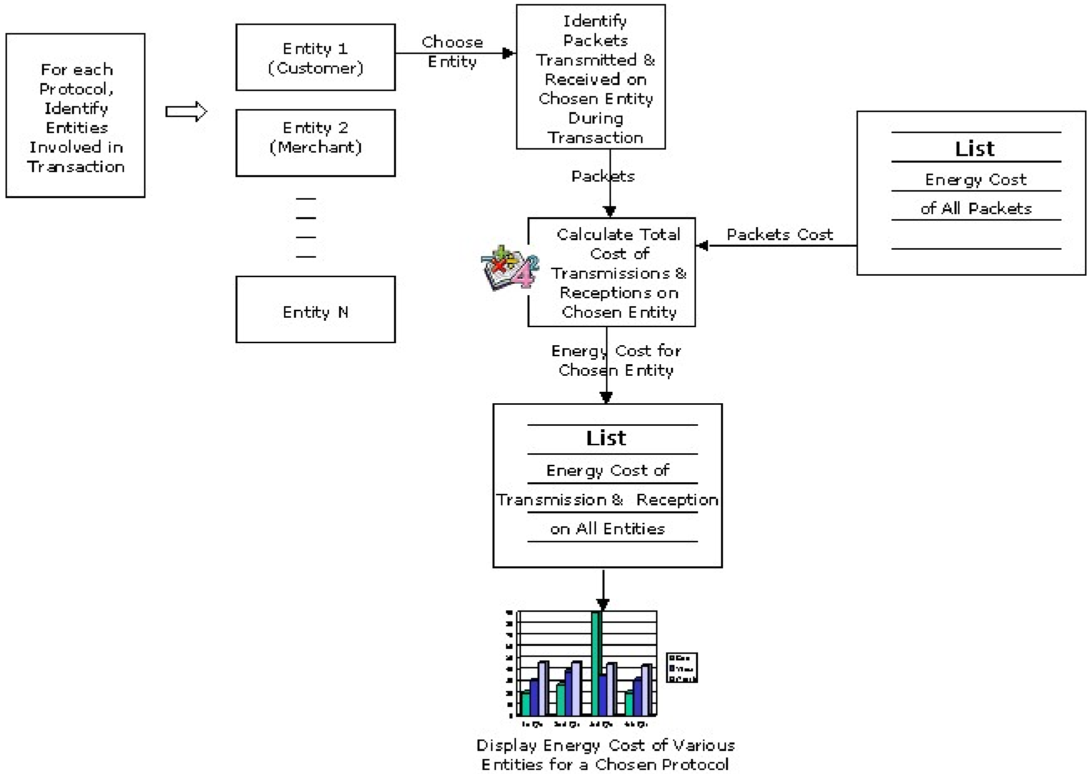

Figure 2: Methodology Architecture Phase 2

2.1.3. Phase 3 (Methodology for Computation of Energy Cost for Each Protocol)

Besides evaluation of protocols in terms of calculation of energy cost for individual entities in a given protocol, the basic motive of this paper is to compare various protocols for their energy requirements. Less energy a protocol consumes, more appropriate it is for M-commerce. In Phase 3 of this paper, the protocol each protocol is chosen individually for calculation of its energy requirements. We have already calculated energy cost of transmissions and receptions for all the entities in a protocol. In this phase, calculations are made to cumulate all the transmissions and reception costs of all the entities involved in a given protocol. A list containing energy cost of all the protocols can be maintained while these statistics are drawn as a graph and discussed in Section 3.

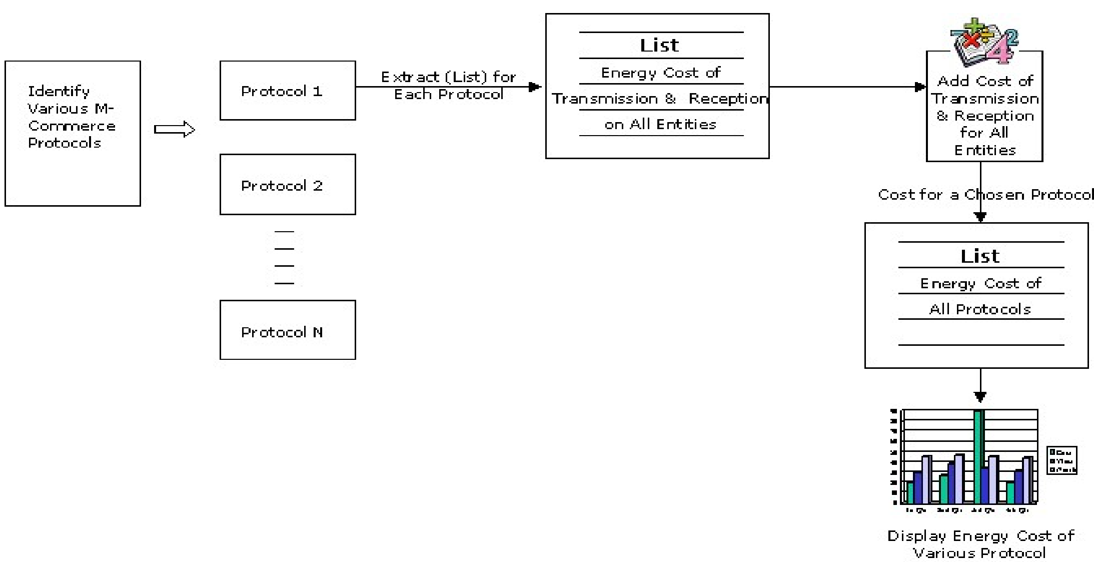

Figure 3: Methodology Architecture Phase 3

2.2. Explanation of Energy Equation & Parameters

First part of this section i.e. 2.2.1 describes the energy equation for transmission and reception that are used to calculate the energy cost for each protocol while the same part describes notations used in this paper as well. The second section 2.2.2describes the realistic assumptions to be used in my work and also gives various parameter values based on literature and assumptions.

2.2.1. Energy Equations & Notations

Mobile devices have several resource constraints including memory, battery power and processing. With battery-constrained mobile devices, it becomes important to use the techniques and algorithms that consume less energy. The energy consumed during the M-commerce payments on a mobile device using direct communication model as per D. Song [4] conventional equation is:

$$E_{elec}B + E_{amp}B(d)^2$$

Where E_{elec} is circuitry energy, E_{amp} is energy it needed to transmit the packet, d is the distance between mobile devices and B is the total number of bits being transmitted. In the same way, the total cost of receiving a data packet by a device is:

$$E_{elec}B$$

Table 1: Gives a short description of the notations used in our paper.

Table 1: Parameters Description

Notation	Description
K	Key for Encryption and Decryption
B	Total Numbers of bits
d	Distance
E_{amp}	Amplification energy constant T_x
E_{elec}	Circuitry Energy constant R_x
ID	Identity (which may be of customer, vendor etc)
N	Nonce
Date	Date of the transaction
Time	Time of the transaction
NIDC	Nick names of the customers
TC	Card Type
Stt	Status
TID	Transaction Identity contains time and date.
VID	Vendor Identity
MAC	Message Authentication Code
H	Hash function
M	Message
CCBrand	Credit Card Brand
CERT	Certificate of the entities

PI	Product Information is composed of the concatenation of amount, ID_{Tran} and credit card data.
OI	Composed of the concatenation ID_{TRAN}, ID_{Brand}, date, N_M, Nc.
Credit card data	Composed of name, expiry, card no, valid from, PIN, Billing address.
DS	Digital Signature
Acc_{inf}	Account number, and sort code.
ID_{Brand}	Credit card brand identifier.
i, j	Counters
Credit card data	Credit card no, expiry date, and PIN.
R	Random number
DESC	Payment Description include delivery address, purchase order no, and date.
Received	Payment receivable updates status, which may include the received payment amount.
$INVOICE_{Req}$	Invoice request includes customer name, merchant name, customer identity and merchant identity.
$CUST_{URL}$	Customer Uniform Resource Locator
Echeq	Electronic cheque consists of Customer ID, Customer certificate, amount and expiry date

2.2.2 Assumptions and Parameter Values

This sub-section initially gives (in Table 2) various realistic assumptions on parameter values to be used for energy calculation in this paper while later on (in Table 3), list of parameter values has been provided along with the sources where these values have been taken from.

Table 2: Assumptions on parameter values

Assumptions	**Parameters**	**Values(bits)**
Assumption **1**	I assume that mobile devices are on average 50 meters distance from radio tower.	
Assumption **2**	Date, time, Price or Amount, R and Received	**64 bits**
Assumption **3**	CC_{Brand},$TID_{Req,}$ ID_{Brand},$VID_{Req,}$ and ACC_{inf}	**128 bits**
Assumption **4**	NID_C, TID and Credit card data	**256 bits**
Assumption **5**	CISec, CVSec, i, j, and VPSec	**32 bits**
Assumption **6**	DESC, and $CUST_{URL}$	**512 bits**
Assumption **7**	$INVOICE_{Req}$	**296 bits**

Authors in reference [5] paper have calculated the values of E_{amp} and E_{elec} are respectively equal to 0.0001μJ/bit/m^2 and 0.05μJ/bit. We assume average d (distance) of mobile devices from radio tower as 50 meters, while the rest of the parameters and their values are shown in the below table. In some cases, parameter values are taken from references and thus mentioned accordingly.

Table 3: Parameters & their Values

Parameter	Value (bits)	Assumptions &References
ID	20	[6]
N	160	[7]
K	256	[8]
Date	64	Assumption 2
Time	64	Assumption 2
NID_C	256	Assumption 4
TC	128	Assumption 3
Stt	64	Assumption 2
TID	256	Assumption 4
VID_{Req}	128	Assumption 3
MAC	128	[9]
H	160	(POPESCU, 2008)
M	160	[10]
CC_{Brand}	128	Assumption3
CERT	4096	[11]
Amount or Price	64	Assumption 2
Credit card data	256	Assumption 4
DS	1024	[12]
ACC_{info}	128	Assumption 3
TID_{Req}	128 bits	Assumption3
VID_{Req}	128 bits	Assumption3
CISec	32	Assumption5
ID_{Brand}	128	Assumption 3
CVSec	32	Assumption 5
I	32	Assumption5
J	32	Assumption 5
VPSec	32	Assumption 5
Timestampe	96	[12]
R	64	Assumption 2
DESC	512	Assumption 6
Received	64	Assumption 2
$INVOICE_{Req}$	296	[6] & Assumption 7
$CUST_{URL}$	512	Assumption 6
ECheq	4244	[6], [11] & Assumption 2
PI	576	Assumptions 2, 4
OI	768	[7], Assumptions 2, 3, & 4

3. Energy Consumption Analysis of Mobile Payment Protocols

This section is the most important section of the paper as it calculates the energy consumption of protocols in order to find out the best one. The energy consumptions calculations here in this section are on the basis of the communication model presented by D. Song [4] as described in the previous section. This section calculates the energy consumption for each step and entity individually of the entities involve in the mobile payment protocol by using equation

$$E_{elec}B+E_{amp}B(d)^2$$

which is used for transmission, while

$$E_{elec}B$$

is used to calculate the energy of receiving bits.

This section is divided into two major sections. Section 3.1 finds the energy consumption of each step and entity involves in the protocol to complete the mobile payment process. The last section 3.2 compares energy cost of protocols in order to find the most optimal protocol for the mobile payment system.

3.1. Energy Consumption Analysis of Protocols

This section is also divided into four sub-sections, each of which is carrying energy consumption calculations of different mobile payment protocol. The below four sub-sections energy consumption not only calculates the overall system energy consumption, but also it finds the energy consumption of each step involved in mobile payment protocol.

3.1.1. Energy Calculation of SPPSKCMS

This section calculates the energy consumption for all the steps involved in the protocol. This protocol is using symmetric key based approach to exchange information securely among different parties [13]. The customer, vendor, payment Gateway, Issuer and Acquire Parties are the entities involved in payment system and in the work to follow, these entities would be represented by C, V, P, I and A respectively. In the mathematical work below, ‘a’ is being used for the energy consumed during packet-transmission while ‘b’ is the energy consumed at mobile device during packet-reception. The payment process as a whole takes 12 steps (transmissions and receptions) among different entities to complete the payment process and energy consumed by each step can be calculated as follows in the table 4.

Table 4: Energy Consumption Calculation of Each Step Involved in SPPSKCMS

Steps		**Name of Party**	**Energy Finding Equations**	**Energy Consumption Per Step**
3	a	C	$0.05*544 + 0.0001*544(50)^2$	**= 163.2** μJ
	b	V	0.05*544	**= 27.2** μJ
4	a	V	$0.05*276 + 0.0001*276(50)^2$	**= 82.8** μJ
	b	C	0.05*276	**= 13.8** μJ
5	a	C	$0.05*1152 + 0.0001*1152(50)^2$	**= 345.6** μJ
	b	V	0.05*1152	**= 57.6** μJ
6	a	V	$0.05*1128 + 0.0001*1128(50)^2$	**= 338.4** μJ
	b	P	0.05*1128	**= 56.4** μJ
7	a	P	$0.05*1076 + 0.0001*1076(50)^2$	**= 322.8** μJ

	b	I	0.05*1076	**= 53.8** μJ
8	a	I	$0.05*608 + 0.0001*608(50)^2$	**= 182.4** μJ
	b	P	0.05*608	**= 30.4** μJ
9	a	P	$0.05*744 + 0.0001*744(50)^2$	**= 223.2** μJ
	b	A	0.05*744	**= 37.2** μJ
10	a	A	$0.05*244 + 0.0001*244(50)^2$	**= 73.2** μJ
	b	P	0.05*244	**= 12.2** μJ
11	a	P	$0.05*768 + 0.0001*768(50)^2$	**= 230.4** μJ
	b	V	0.05*768	**= 38.4** μJ
12	a	V	$0.05*384 + 0.0001*384(50)^2$	**= 115.2** μJ
	b	C	0.05*384	**= 19.2** μJ

The energy consumption of each party involved in the entire process can be represented by table 5.

Table 5: Energy Consumption Calculation of Each Party Involved in SPPSKCMS

Party Name	**No's of Steps**	**Total Energy Consumption**
C (Customer)	3a + 4b + 5a + 12b	**= 541.8** μJ
V (Vendor)	3b + 4a + 5b + 6a + 11b + 12a	**= 659.6** μJ
P (Payment Gateway)	6b + 7a + 8b + 9a + 10b + 11a	**= 875.4** μJ
I (Issuer)	7b + 8a	**= 236.2** μJ
A (Acquire)	9b + 10a	**= 110.4** μJ

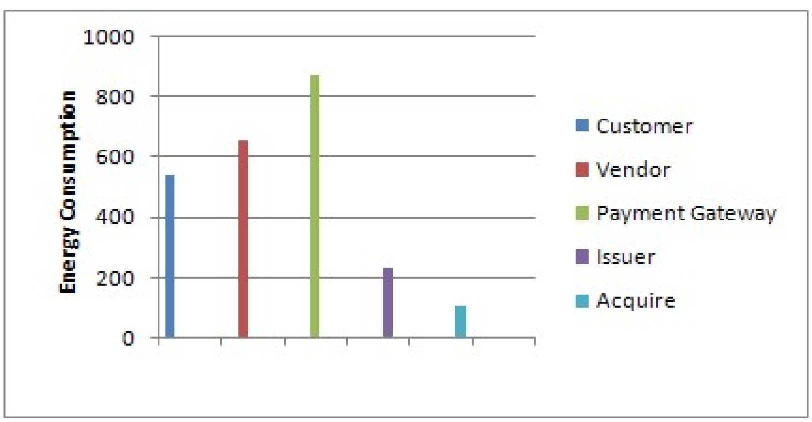

Figure 4: SPPSKCMS Protocol Energy Consumption by Each Party

Now total energy consumed by the system by using this protocol can be calculated as:

Overall System Energy Consumption = C+V+P+I+A = 2423.4 μJ

3.1.2. Energy Calculation of SET

This section calculates the energy consumption for all the steps involved in SETprotocol [14]. It uses secure channels for communications that provide more payment security. It is not only secure but also uses well organized authentication technique for authentication purposes. The customer, Merchant and Payment Gateway entities are used to complete the whole payment process. In the mathematical work below C, M and G represent customer, merchant and payment gateway respectively. There are six steps involved in managing the payments and energy consumed in each of the steps can be calculated as follows in table 6.

Table 6: Energy Consumption Calculation of Each Step Involved in SET

Steps	Name of Party	Energy Finding Equations	Energy Consumption Per Step
1 a	C	$0.05*308 + 0.0001*308(50)^2$	**= 92.4** μJ
b	M	$0.05*308$	**= 15.4** μJ
2 a	M	$0.05*9216 + 0.0001*9216(50)^2$	**= 2764.8** μJ
b	C	$0.05*9216$	**= 460.8** μJ
3 a	C	$0.05*8192 + 0.0001*8192(50)^2$	**= 2457.6** μJ
b	M	$0.05*8192$	= **409.6** μJ
4 a	M	$0.05*11616 + 0.0001*11616(50)^2$	=**3484.8** μJ
b	G	$0.05*11616$	= **580.8** μJ
5 a	G	$0.05*6912 + 0.0001*6912(50)^2$	= **2073.6** μJ
b	M	$0.05*6912$	= **345.6** μJ
6 a	M	$0.05*6784 + 0.0001*6784(50)^2$	= **2035.2** μJ
b	G	$0.05*6784$	= **339.2** μJ
7 a	G	$0.05*5376 + 0.0001*5376(50)^2$	= **1612.8** μJ
b	M	$0.05*5376$	= **268.8** μJ

The energy consumption of each party involved in the entire process can be represented by table 7.

Table 7: Energy Consumption Calculation of Each Party Involved in SET

Party Name	No's of Steps	Total Energy Consumption
C (Customer)	1a + 2b + 3a	**= 3010.8** μJ
M (Merchant)	1a + 2a + 3b + 4a + 5b + 6a + 7b	**= 9324.2** μJ
G (Gateway)	4b + 5a + 6b + 7a	**= 4606.4** μJ

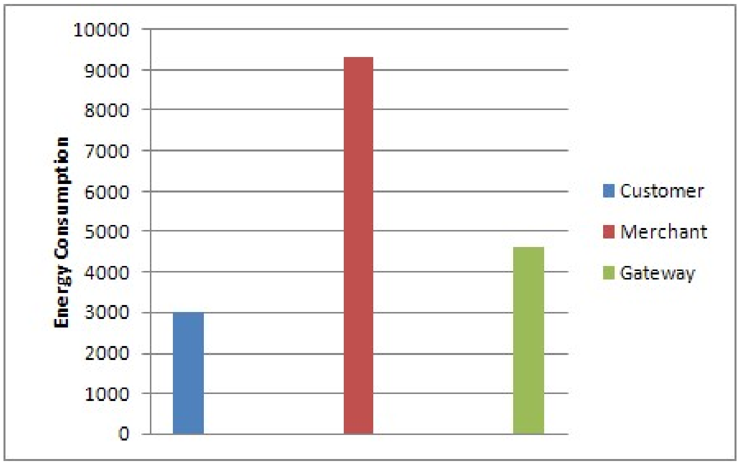

Figure 5: SET Protocol Energy Consumption by Each Party

Now total energy consumed by the system by using this protocol can be calculated as:

Overall System Energy Consumption = C+M+G = 16941.4 μJ

3.1.3. Energy Calculation of Privacy in New Mobile Payment Protocol (PNMPP)

This section calculates the energy consumption for the steps involved in Privacy in New Mobile Payment Protocol [15]. It is based on client-centric model and the payer manages transaction. The process includes Payer, Payee, Payers MNO, Payees MNO and TSL to manage the payment transaction process. It needs 13steps to complete the payment process and the energy consumption in each of the steps can be calculated in the table 8.

Table 8: Energy Consumption Calculation of Each Step Involved in Privacy in New Mobile Payment Protocol

Steps	Name of Party	Energy Finding Equations	Energy Consumption Per Step
1 a	Payer	$0.05*340 + 0.0001*340(50)^2$	= **102** μJ
b	Payee	0.05*340	= **17** μJ
2 a	Payee	$0.05*296 + 0.0001*296(50)^2$	**= 88.8** μJ
b	Payer	0.05*296	**= 14.8** μJ
3 a	Payer	$0.05*1436 + 0.0001*1436(50)^2$	= **430.8** μJ
b	Payers MNO	0.05*1436	= **71.8** μJ
4 a	Payers MNO	$0.05*160 + 0.0001*160(50)^2$	= **48** μJ
b	TSL	0.05*160	= **8** μJ
5 a	TSL	$0.05*96 + 0.0001*96(50)^2$	= **28.8** μJ
b	Payers MNO	0.05*96	= **4.8** μJ
6 a	Payers MNO	$0.05*1044 + 0.0001*1044(50)^2$	= **313.2** μJ
b	Payees MNO	0.05*1044	= **52.2** μJ
7 a	Payees MNO	$0.05*1536 + 0.0001*1536(50)^2$	= **460.8** μJ

b	Payee	0.05*1536	= **76.8** µJ
8 a	Payee	$0.05*928 + 0.0001*928(50)^2$	= **278.4** µJ
b	Payees MNO	0.05*928	= **46.4** µJ
9 a	Payees MNO	$0.05*160 + 0.0001*160(50)^2$	= **48** µJ
b	TSL	0.05*160	= **8** µJ
10 a	TSL	$0.05*96 + 0.0001*96(50)^2$	= **28.8**µJ
b	Payees MNO	0.05*96	= **4.8**µJ
11 a	Payees MNO	$0.05*832 + 0.0001*832(50)^2$	= **249.6** µJ
b	Payers MNO	0.05*832	= **41.6** µJ
12 a	Payers MNO	$0.05*928 + 0.0001*928(50)^2$	= **278.4** µJ
b	Payer	0.05*928	= **46.4** µJ
13 a	Payees MNO	$0.05*544+ 0.0001*544(50)^2$	= **163.2** µJ
b	Payee	0.05*544	= **27.2** µJ

The energy consumption of each party involved in the entire process can be represented by table 9.

Table 9: Energy Consumption Calculation of Each Party Involved in Privacy in New Mobile Payment Protocol

Party Name	**No's of Steps**	**Total Energy Consumption**
Payer	1a + 2b + 3a + 12b	= **594** µJ
Payee	1b + 2a + 7b + 8a +13b	= **488.2** µJ
Payers MNO	3b + 4a + 5b + 6a + 11b +12a	= **757.8** µJ
Payees MNO	6b + 7a + 8b + 9a +10b +11a + 13a	= **1025** µJ
TSL	4b + 5a + 9b + 10a	= **73.6** µJ

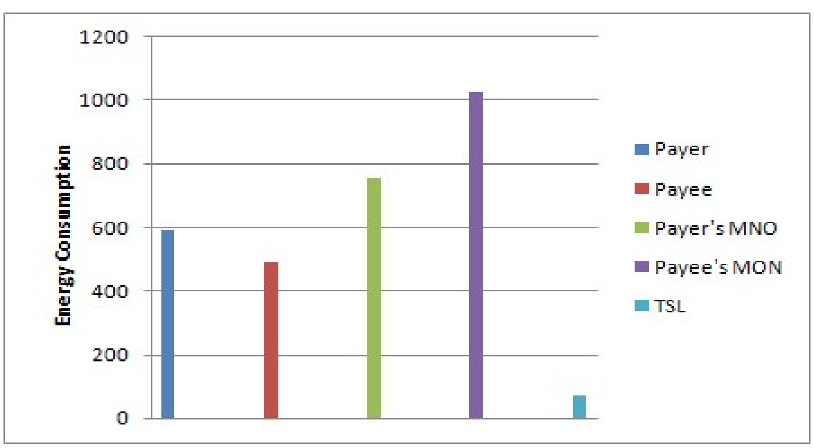

Figure 6: Privacy in New Mobile Payment Protocol Energy Consumption by Each Party

Now total energy consumed by the system by using this protocol can be calculated as:

Overall System Energy Consumption = Payer + Payee + Payers MNO + Payees MNO + TSL = 2938.6 µJ

3.1.4. Energy Calculation of SSMCP*

This section calculates the energy consumption for the steps involved in SSMCP*protocol [14]. SSMCP* uses TSL client authentication or WTLS class 3, which provide more reliable, secure and authenticated services for receiving e-cheque payments. Comparatively, it requires less number of steps to complete the e-cheque payment process and energy consumed by each step can be calculated as follows in table 10.

Table 10: Energy Consumption Calculation of Each Step Involved in SSMCP*

Steps		Name of Party	Energy Finding Equations	Energy Consumption Per Step
1	a	C	$0.05* 5576 + 0.0001*5576(50)^2$	= **1672.8** µJ
	b	M	0.05*5576	= **278.8** µJ
2	a	M	$0.05*1480 + 0.0001*1480 (50)^2$	= **444** µJ
	b	C	0.05*1480	= **74** µJ
3	a	C	$0.05*10196 + 0.0001*10196(50)^2$	= **3058.8** µJ
	b	B	0.05*10196	= **509.8** µJ
4	a	B	$0.05* 5268 + 0.0001*5268(50)^2$	= **1580.4** µJ
	b	C	0.05*5268	= **263.4** µJ
5	a	B	$0.05* 9364 + 0.0001*9364(50)^2$	= **2809.2** µJ
6	a	M	0.05*9364	= **468.2** µ

The energy consumption of each party involved in the entire process can be represented by table 11 as:

Table 11: Energy Consumption Calculation of Each Party Involved in SSMCP*

Party Name	No's of Steps	Total Energy Consumption
C (Customer)	1a + 2b + 3a + 4b	= **5069** µJ
M (Merchant)	1b + 2a + 6a	= **1191** µJ
B (Bank)	3b + 4a + 5a	= **4899.4** µJ

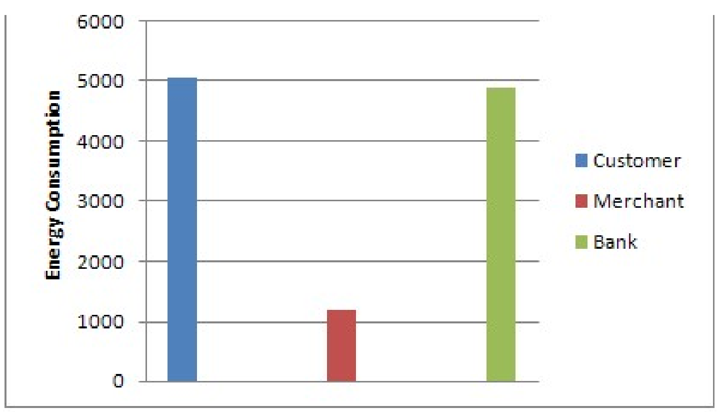

Figure 7: SSMCP* Energy Consumption by Each Party

Now total energy consumed by the system by using this protocol can be calculated as:

Overall System Energy Consumption = C + M + B = 11159.4 μJ

4. Final Results & Discussion

Figure 8 below shows the comparison of all four protocols and the purpose of this comparison is to analyze the energy requirements of these protocols during mobile payment process. Based on the calculations in the previous section, and an insight into the figure below, SET protocol consumes maximum mobile battery amongst all other protocol in discussion. As a matter of fact, it consumes eight times more battery power than the lowest energy consuming protocol i.e. SPPSKCMS. Similarly, SSMCP* also consumes rather considerable battery resources, and hence would not become an appropriate choice for the M-commerce payment system on resource-constrained mobile devices. “Privacy in new mobile payment protocol” has the closest results to SPPSKCMS protocol in terms of battery consumption. Hence through our analysis of energy requirements, we recommend the SPPSKCMS for mobile-based commerce payment systems as it does not only consume less energy but it is also much secure than other competitors. Table 12 and figure 8 show the energy consumption comparison of protocols as below.

Table 12: Energy Consumption Comparison of Protocols

Protocol Name	**Total Energy Consumption**
SPPSKCMS Protocol	**2423.4 μJ**
SET Protocol	**16941.4 μJ**
PNMPP Protocol	**2938.6 μJ**
SSMCP* Protocol	**11159.4 μJ**

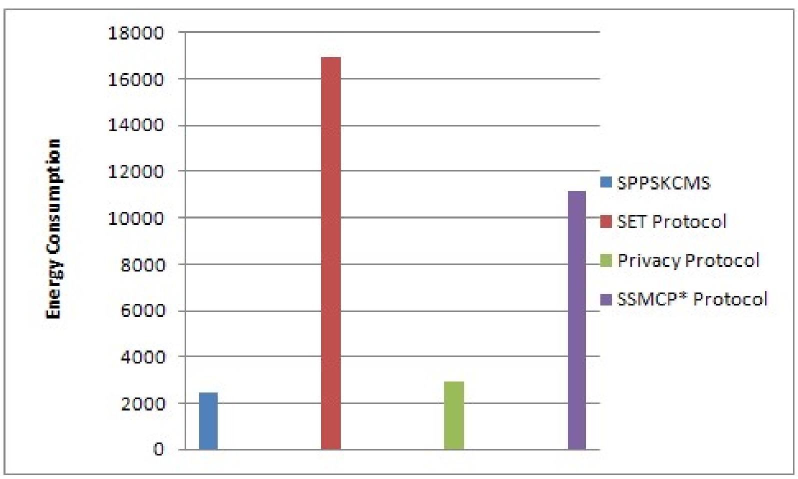

Figure 8: Energy Consumption Comparison of all Four Protocols

5. Conclusion

This paper presented an energy consumption analysis of four mobile payment protocols based on the conventional energy consumption model of D. Song [4] Mathematical computations give a three-stage energy consumption analysis. Level 1 of the computations give per-packet energy consumption, level 2 computes per-entity energy consumption while level 3 computes overall energy consumption for selected M-commerce payment protocols. This paper holds true for direct model of communication among different entities involved in the mobile payment protocols. One of the major outcomes of this paper is that it unveils energy efficient and energy intensive M-commerce payment protocols. In addition, this paper also computes power consumption for each entity of the mobile payment protocol.

Besides revealing power consumption, it also reflects the actual load of traffic (in terms of packets transmitted and received) on individual entities.

It is concluded that SET performs worst in terms of energy consumption during an M-commerce payment transaction as it consumes highest system energy during the mobile payment. The 2nd worst protocol is the SSMCP. Although it is consuming approximately 35% less energy as compared to SET, but still we think it may not be appropriate for the entities involved in M-commerce payment protocol specifically for the mobile devices. The2nd best is based on the computations is Privacy in new Mobile Payment Protocol (PNMPP), which consumes almost 82% less energy as compare to SET. The SPPSKCMS is the overall best as it consumes the lowest energy of all protocols.

It means that SPPSKCMS consume almost 85% less energy as compare to the SET. Although SPPSKCMS is consuming lesser energy as compared to other protocols, its energy consumption levels are very close to 'Privacy in new Mobile Payment Protocol'. Though SPPSKCMS leads by difference of just 3% and that matters a lot in terms of resource constrained mobile devices. Finally, regarding this paper, it is concluded that the SSPSKCMS is more appropriate protocol for M-commerce payments in terms of battery power consumptions. Thus, it is the most recommended protocol based on our computations and this should be used as mobile payment protocol on mobile payment devices. Privacy in new Mobile Payment Protocol (PNMPP) could also be used as an alternate option because it is only 3% less in battery usage performance as compared to SPPSKCMS.

6. Future Work

Literature may provide many studies on security issues of the selected four protocols. As there is a narrow difference between the energy consumption performance of SPPKCMS and PNMPP, both could be alternatively used if the preference criterion is the energy consumption only. In this situation, it would be ideal to use the protocol with better security performance and thus a thorough security analysis of both SPPKCMS and PNMPP should be conducted.

This paper comprises of the energy consumption analysis of four most renowned M-commerce payment protocols. Study of literature may reveal other interesting mobile payment protocols like 3-D Secure Protocol etc. Thus, energy consumption analysis of various other protocols may produce some interesting results.

Results in this research have been computed using renowned energy equations by D. Song [4]. There are various other alternative computational mechanisms and energy equations by other authors that could be utilized to compute energy cost of protocols. Adopting any of the alternatives may enable us to compare results acquired in this paper with the ones computed though any other mechanisms. Doing so will not only provide verification of the current work but is also expected to reveal interesting results.

Level 1 of the computations under this research provides us with per-step (i.e. per-packet) energy consumption. Thorough security analysis of these protocols may help in identification of some irrelevant steps (i.e. unimportant transmissions and receptions) in future thus considerably reducing the energy cost of each protocol.

In Level 2 of the computations under this paper provides with per-entity based energy consumption. Computation at this level initiates through identification of packets transmitted and received at each node and thus with a minimal effort in future, load on each entity (in terms of packets transmitted and received) could be acquired. Such findings may pave the way to compute statistics like processing cost of a protocol in future.

References

[1] S. Banzal, "Mobile Banking & M–Commerce and Related Issues", Technical Report, October 2008

[2] H.H. Lin and Y. Sang, "An examination of the determinants of customer loyalty in mobile commerce contexts", Information & Management (Elsevier Journal) 43 (2006) 271–282

[3] H. Eren, “Wireless Sensors and Instruments Networks, Design, and Applications”, By Taylor & Francis Group, LLC, 2006, pp. 211-212

[4] D. Song, “Probabilistic Modeling of Leach Protocol and Computing Sensor Energy Consumption Rate in Sensor Networks”,CS Department, Texas A&M University, Technical Report: TR 2005-2-2. February 22, 2005

[5] W.R. Heinzelman, A. Chandrakasan, and H. Balakrishman, “Energy-Efficient Communication Protocol for Wireless Microsensor Networks”, Published in the IEEE Proceedings of the Hawaii International Conference on System Sciences, January 4-7, 2000, Maui, Hawaii.

[6] W. Ham, H. Choi, Y.Xie, M.Lee and K. Kim, “ Secure one-way mobile payment system keeping low computation on mobile devices”, in The Third International Workshop on Information Security Applications (WISA 2002). pp. 287-307

[7] Q. Li, X. Zhang, J.P. Seifert andH. Zhong, “Secure Mobile Payment via Trusted Computing”, IEEE Third Asia-Pacific Trusted Infrastructure Technologies Conference, 2008

[8] J. Gao, V. Kulkarni, H. Ranavat, L. Chang, and H. Mei “A 2D Barcode-Based Mobile Payment System”, Multimedia and Ubiquitous Engineering, Third International IEEE Conference, 2009

[9] C. Karlof, N. Sastry, and D.Wagner, “TinySec: A Link Layer Security Architecture for Wireless Sensor Networks”, SenSys 04 Proceeding of the 2nd International Conference on Embedded Networked Sensor Systems, 2004. p.p. 162-175

[10] K. Piotrowski, P. Langendorferand D. Kulikowski,“Moneta: An Anonymity Providing Lightweight Payment System for Mobile Device”, Available from: http://VirtualGoods.tu-ilmenau.de/2004/MONETA.pdf

[11] Fpkipa, “X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program Federal”, Federal PKI Policy Authority Shared Service Provider Working Group, January 7, 2008.

[12] M. Hassinen, “Studies in Mobile Security”, Doctoral dissertation, Kuopio University Publication H. Business and Information Technology, 10.2007.

[13] J.A. Tellez, J.M. Sierra, A. Izquierdoand M. Carbonell, “A secure protocol for a payment system based on a kiosk centric case mobile scenario”, ICCSA 2006, LNCS 3984, pp. 798–807, 2006.

[14] E. Haddadand B. King, “A Simple Secure M-Commerce Protocol SSMCP*”, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, March 2007

[15] T.S. Fun, Y. Bengl, R. Roslan, &S. Habeeb, “Privacy in New Mobile Payment Protocol”, World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering Vol:2, No:11, 2008

[16] Munir Hussain et al., “Technical Evaluation of the Functionality of Popular Mobile Payment Protocols”, In IOARP Journal of Communication and Networks, Volume 2, Issue 1, June 2017.