Send Orders for Reprints to reprints@benthamscience.ae

98 *The Open Cybernetics & Systemics Journal,* 2014, *8,* 98-103

Open Access

Authenticated Key Agreement Protocol for Wireless Sensor Networks

Zhang Li[1,*], Xie Bin[2], He Z. Qiang[3] and Jin Y. Quan[4]

Institute of Computer Application, China Academy of Engineering Physics, Sichuan, China, 621900.

Abstract: In order to solve the excessive computation and storage requirement arising due to the frequent sensor nodes movement in WSN, a new public key has been proposed based on ECC key agreement protocol. The mutual authentication and agreement on a session key can be realized between users, or between user and a network server in WSN. This protocol adopts ECC techniques to consult session keys and AES Symmetrical encryption technology to achieve confidentiality. Compared with traditional protocol, this protocol could provide greater security with relatively fewer bits and reduce the requirement of computation and storage. A protocol has been proved to be a secure authenticated key agreement in ID-BIM models. Results show that it provides a perfect forward/back secrecy and PKG forward secrecy.

Keywords: ECMQV, ECDH, ID-BIM, key agreement, security, wireless sensor networks.

1. INTRODUTION

Wireless sensor network [1] is a kind of typically distributed mobile network composing of many tiny sensory nodes deployed in the testing area. The WSN network is composed of small memory storage, limited computation ability and limited power energy. The traditional network key agreement protocols are not completely suitable for WSN. So it is necessary to find a safe and efficient key agreement protocol to meet the security requirements of WSN.

Currently, research on key agreement protocol for WSN includes identity-based key system and certificate-based key system. Shamir [2] proposed an identity-based cryptography system, and some identity-based key agreement protocols [3] for WSN. Researchers generally accepted that symmetric encryption algorithm combined with key pre-distribution model for key distribution management [4-7] is efficient. Because of the sensor network nodes with limited resources, certificate based key management schemes and public key cryptography has been considered as not a suitable for WSN for a long time. However, recent researches show that the algorithm based on Elliptic Curve Cryptography can be operated efficiently in wireless sensor nodes [8]. Neal Koblitz and VS Miller first proposed the public key cryptosystem [9, 10] (ECDH), based on the elliptic curve to achieve DH algorithm. LAW *et al.* [11] proposed a key exchange protocol based on ECDH (ECMQV) , ECMQV protocol can efficiently achieve mutual authentication and agreement on a session key. With implicit authentication, it can effectively reduce the cost of communication and computation. Some ECC based protocols for WSN were put forward [12, 13]. A comparison of DH and ECDH shows that, to achieve the same security, ECDH key agreement Algorithm needs operate more efficiently, compute faster and require shorter key and less memory storage.

Moreover, researches at Brazil UNICAMP University have been the first to achieve Tate pairing [14] encryption algorithm on sensor nodes based on TinyECC. However, even with Tate pairing encryption, the computation is relatively higher than that of ECC, and it is not suitable for WSN.

Cheng *et al.* [15] proposed a IBE-based key management scheme. In this scheme, ECC cryptography is used to encrypt data, and by ID-based public key it can effectively improve the efficiency of key management [16]. In this paper, A identity authentication key agreement protocol based on ECC is proposed for WSN, which combines ElGamal with ECC cryptography to achieve mutual authentication and agreement on a session key. In this scheme user data is encrypted to provide confidentiality of communication and integrity of the information against temperaments. This protocol can also provide known-key security, forward/back security, PKG forward security. Moreover, it realizes key-update after nodes join/leave and avoids Key Escrow. Meanwhile, this protocol can decrease computing resource.

The rest of this paper is organized as follows: In section 2, prepare knowledge and assumptions related to our work have been discussed. In section 3, WSN model and key management protocols are proposed which include key agreements and updates. Section 4 is security analysis, protocol is proved in ID-BIM security model. Section 5 is agreement performance analysis. Section 6 concludes the paper. Section 7 is Acknowledgement.

2. PREPARE KNOWLEDGE

2.1. ECC Parameter Selection

Let $E:\{a,b,G,N,P\}$ denote ECC parameter, assume ECC equation in finite field $GF(p)(p>3)$ is $E: y^2 = (x^3 + ax + b) \bmod p$, $x, y \in GF(p)$. Where

1874-110X/14 2014 Bentham Open

$a,b \in GF(p)$ and $4a^3+27b^2 \neq 0 (\text{mod } p)$. G denotes a base point for ECC $E/F(P)$, N is rank of G, let $G=(x_G, y_G)$ denote G. Assume user private key is s, public key is sG, $sG=(x_S, y_S)$, $s \in Z_P$。

2.2. Singular Elliptic Eurve

Let p is characteristic of finite field F_q, $q=p$ or $q=2^m$, where m is the prime number.

The number of point in Elliptic Eurve E over finite field $GF(q)$ is $\#E=p^r+1-t, |t| \leq 2\sqrt{p^r}$, where $p^r=q$, t is trace of Elliptic Eurve E in F_q. If $p \mid t$, E is Singular Elliptic Eurve, at this point break elliptic curve is harder than discrete logarithm problem on base field.

2.3. ECDLP

Given Elliptic Eurve $E(F_q)$ over F_q and base point G, N is rank of G:

-Provided x is integer, calculate $Q=xP$ is simply.

-Provided Q, calculate x to satisfy $Q=xP$ is hard.

2.4. ECC-based ElGamal Cryptosystem

-Let $E_q(a,b)$ be a rank of kr, security Elliptic Eurve where k is small integer and r is a large prime.

-The point G in Elliptic Eurve $E_q(a,b)$ is of order r.

-Generate a random a where $(1<a<r)$, calculate $P=a \cdot G$.

-Public key: $k'=(P,G)$, let (m_1, m_2) denote plaintext, Encryption algorithm as follow:

Generate a secret integer $l(0<l<r)$, calculate

$R=l \cdot G$, $(x,y)=l \cdot P$, $C=(xm_1, ym_2)$, ciphertext is (R,C).

-Private key: $k''=a$, Decryption algorithm: calculate $(x,y)=a \cdot R$, $m_1=x^{-1} \cdot xm_1, m_2=y^{-1} \cdot ym_2$, recover plaintext (m_1, m_2).

2.5. ECDH Hypothetical Problem

Definition 1 ECDH

Provide (s,p,G,z), determine $zG=spG$ or not, where the point G denote a base point for $E/F(P)$, $s,p,z \in Z_p$.

2.6. ID-BIM Model

Chen *et al.* [6] define formal security model for the identity-based authenticated key agreement protocol (ID-BIM model).

Authenticated key agreement protocol in this model possesses the following security attributes such as Known-key security, Forward secrecy, Key-compromise impersonation, Unknown key-share resilience and Key control [17].

The model includes a set U for protocol participants and an adversary E. Each participant is modeled by oracle $\prod_{A,B}^{n}$, which simulates a participant A carrying out a protocol session in the belief that it is communicating with another participant B for nth time (*i.e.* the nth run of the protocol between A and B). An adversary E, which is a probabilistic polynomial time Turing Machine and it has access to the participants' oracles. E can only relay, modify, delay, interleave or delete messages. For any pair of oracles $\prod_{A,B}^{n}$ and $\prod_{B,A}^{n}$, E is called the benign adversary on these two oracles if it simply passes messages to and fro between the participants, A and B. We note that all communications go through the adversary. Participant oracles only responds to queries by the adversary and do not communicate directly amongst themselves. It is assumed that E is allowed to make the following three types of queried of the oracles:

-Send: This allows E to send a message of its choice to the oracle, say $\prod_{A,B}^{n}$, in which case participant A believes the message has been sent by participant B. E may also initiate a protocol run between two participants, A and B.

-Reveal: this allows E to ask a particular oracle to reveal the session keys (if any) it currently holds for E.

-Corrupt: This allows E to ask a particular oracle to reveal its long-term private key and to replace the key pair with a key of E's choose.

An oracle exists in one of the following several possible states:

-Accepted: an oracle is accepted if it decides to accept, holding a session key, after the receipt of properly formulated messages.

-Rejected: an oracle is rejected if it decides to reject holding a session key.

-*: an oracle is * if it has not made any decision to accept or reject.

-Opened: an oracle is opened if it has answered a relevant query.

-Corrupted: an oracle is corrupt if it has answered a corrupt query.

For attacking a protocol, E performs an experiment with a set of selected oracles. During the experiment E asks a polynomial bounded, number of queries (including Send, Reveal and Corrupt) from the oracles and finally makes a Test query for the chosen oracle. The oracle, say $\prod_{A,B}^{n}$ to

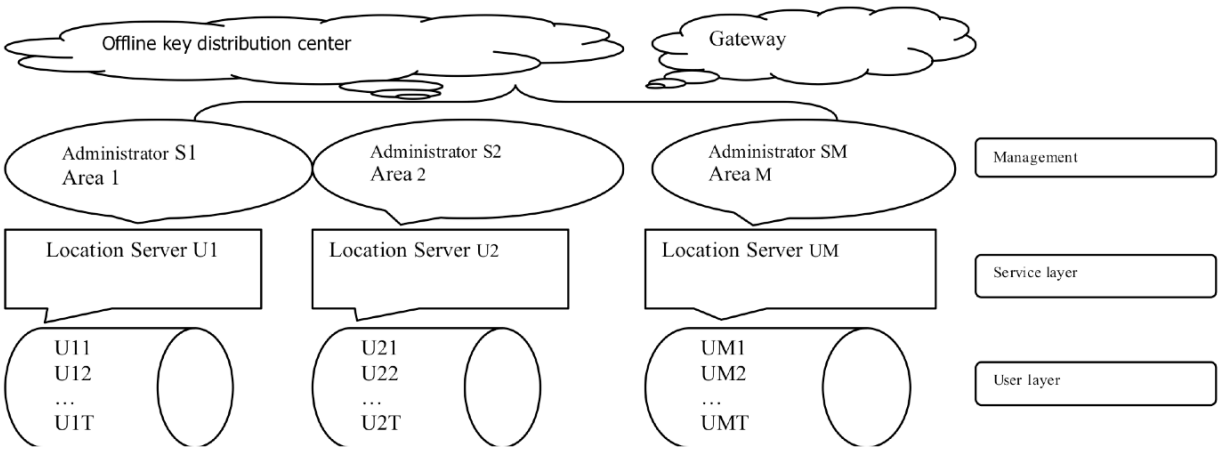

Fig. (1). WSN model.

be chosen for answering the Test query must be accepted, be unopened and neither A or B can be corrupted. Furthermore, there must be no open oracle $\prod_{A,A}^{n}$ with which it has had a matching conversation. To answer the query, the oracle flips a fair coin $b \in \{0,1\}$, and returns the session key if $b=0$, otherwise a random key is sampled from $\{0,1\}^k$ it $b=1$. Then E has to guess b. E's advantage, denoted by advantage $Adv^E(l)$, is the probability that E can distinguish the session key held by the queried oracle from a random string, and it is defined as:

$$Adv^E(l) = \left| 2\Pr\left[b' = b\right] - 1 \right|,$$

Definition 2

A protocol is a secure authenticated key agreement with key confirmation protocol if:

-In the presence of the benign adversary on $\prod_{A,B}^{n}$ and $\prod_{B,A}^{n}$, both oracles always accept holding the same session key. And this key is distributed uniformly and randomly on the equation: $\{0,1\}^k$.

-The probability of $Adv^E(l)$ is negligible.

3. PROPOSED PROTOCOL

In this paper, WSN model is shown in Fig. (**1**).

Assume WSN network is divided into three layers: management, service, and user. This scheme gives the key agreement protocol for key agreement of each layer

This protocol is based on the framework of literature [14]. Several assumptions made in this paper include:

-Users can effectively operate the encryption and decryption algorithm.

-Users can select updated parameters from Z_P.

-Effective attack cannot occur during the initial deployment phase.

-In the deployment phase, the attacker can only intercept a small part of the link information.

1) Key agreement protocol

Assume user A and B, after implementing the key agreement protocol, (shown in Fig. **2**):

Protocol 1

(1) $A \to B : ID_A \| R_A \| \left(x_1 ID_A, y_1 R_A\right)$

(2) $B \to A : ID_B \| R_B \| E_K\left(R_A \| ID_A \| bsGy_2 \| \left(x_1 ID_B, y_1 R_B\right)\right)$

(3) $A \to B : E_K\left(R_B \| ID_B \| asGy_2\right)$

(4) $B \to A : E_K\left(L \| start\right)$

(5) $A \to B : E_K\left(M \| ID_A \| L\right)$

Fig. (2). Authenticated key agreement protocol.

where:

User A: private key *a*, public key $aID_AsG, R_A = F_AsG$, fresh random number F_A.

User B: private key *b*, public key $bID_BsG, R_B = F_BsG$, fresh random number F_B, $a, b, F_A, F_B \in Z_P$.

L is the communication counter, it keep track of the number of times the communication between users as plus 1, when L reached the threshold, update key.

Start is sign of the beginning of communication, K is a session key.

Encryption K extract from x_2, and adopt AES symmetric block technology, y_2 as a signature key.

Protocol described in detail below:

Step 1: A first calculate

$$abID_B sG \cdot ID_B^{-1} = absG = (x_1, y_1)$$

encrypt ID_A, R_A.

Step 2: B calculate

$$baID_A sG \cdot ID_A^{-1} = basG = (x_1, y_1)$$

verify ID_A, R_A, if it is changed, give up session, or calculate

$$(x_2, y_2) = F_A F_B sG = F_A R_B = F_B R_A$$

Session key K extract from x_2 and calculate $bsGy_2$, encrypt information by AES.

Step 3: A calculate

$$(x_2, y_2) = F_A F_B sG = F_A R_B = F_B R_A$$

Decrypt and verify ID_B, R_B, if it is changed, give up session, or verify $bsG = bsGy_2 \cdot y_2^{-1}$, if it is right, a session key between A and B is successful achieve, or give up session.

Step 4: B first verify $asG = asGy_2 \cdot y_2^{-1}$, if it is right, send L and Start to A, or give up session.

Step 5: A send plaintext M, L and ID_A to B.

4. SECURITY ANALYSIS

Initial assumptions must invariably be made to guarantee the success of Protocol **1** (shown in Fig. **2**). We prove that Protocol 1 in ID-BIM model is secure.

Theorem Protocol **1** is a secure authenticated key agreement protocol assuming that ECDH hypothetical problem is hard.

Proof: Condition 1 follows the assumption that the two oracles follow the protocol and E in the benign. In this case, both oracles accept (since they both receive correctly formatted messages from the other oracle) holding the same session key K (since $K_{AB} = K_{BA}$ by the ECC and the matching conversation). Since ECC is a random oracle, K is distributed uniformly at random on $\{0,1\}^k$.

Condition 2 Consider an arbitrary adversary E, and suppose, by the way of contradiction, that $Adv^E(l) = \varepsilon$ is non-negligible. Suppose that there exists an oracle $\prod_{A,B}^n$ -after having a matching conversation to another oracle $\prod_{B,A}^n$ (both A and B have not been corrupted), assume that adversary E can make most q_1 Corrupt queries and q_2 conversations. There exists simulator X that can determine ECDH problem with non-negligible $\varepsilon' = \varepsilon / q_1^2 q_2$.

Suppose the problem on ECDH is (s, p, G, z), X needs to verify $zG = spG$. Initial phase X send (sG, G, p) to adversary to achieve system parameter to calculate sG. Assume X doesn't knows system secret key s, this parameter have the same distribution with real parameter.

At the beginning of simulation, select three random integers: A, B, n. Where $A, B \in \{1, 2, \cdots, q_1\}$, $n \in \{1, 2, \cdots, q_2\}$, let ID_A, ID_B denote Ath and Bth participant. X select queried oracle $\prod_{A,B}^n$. X simulate attack play for adversary E. The process as follows:

-Corrupt: Input ID_i, if $ID_i = s$, Judge ECDH problem with *s*, or if $i \neq A$, calculate

$s_i sG$, $R_i = F_i sG$, $s_i sID_i G$.

Return $(s_i sID_i G, s_i sG)$, where $s_i, F_i, s \in Z_p$. parameter selection of the above follows the real distribution, this attack is efficient for adversary E. If $i = A$ or $i = B$, error exit.

-Send: E respond Send query honestly to all of oracles except $\prod_{A,B}^n$, while respond to $\prod_{A,B}^n$, generate A's and B's public key

$s_A ID_A sG$, $s_B ID_B sG$, $R_A = F_A sG$, $R_B = F_B sG$.

Return A_1, A_2 to oracle $\prod_{A,B}^n$.

where

$$A_1 = s_A ID_A sG, A_2 = zF_A G / p$$

if

$$zG = spG, \ A_2 = zF_A G / p = F_A sG$$

Suppose oracle receives B_1, B_2, then calculate the share key $K_A = K_B = s_A s_B sG$, session key $SK_{AB} = F_A F_B sG$.

-Reveal: While queried oracle is $\prod_{A,B}^n$ or $\prod_{B,A}^n$, error exit. Or return session key.

-Test: During the experiment E choose a oracle to send Test query, if E choose

-The oracle that is queried by X, return session key, or error exit.

Output: Finally, E guess b.

Let T denote the fact that X is not error exit. $\Pr[T] \geq 1/q_1^2 q_2$.

Suppose $zG = spG$, then E can successfully guess b with probability from the equation: $\varepsilon + 1/2$.

If E can achieve b with non-negligible ε, then X can determine $zG = spG$ with non-negligible ε'. In all, $\varepsilon' = \varepsilon / q_1^2 q_2$, then X can judge ECDH problem with the probability of $\varepsilon' = \varepsilon / q_1^2 q_2$. This assumption is contradictory to ECDH. Thu, this assumption is not correct. And hence Protocol **1** is secure.

Protocol 1 can provide forward/back security and PKG forward security. Even if adversary E achieves A's and B's private key and system key, it can only calculate the first share key K, however the session key SK_{AB} need to know F_A, F_B, it is hard to calculate F_A, F_B through $R_A = F_A sG$ and $R_B = F_B sG$.

5. PERFORMANCE ANALYSIS

In this section, the performance of the protocol is analyzed.

Let e_1 denote a computation on elliptic curve, and the cost of sending and receiving a message is e_2 and e_3. The performance of Protocol 1 shown in Table **1**.

As seen from Table **1**, Protocol 1 for each user needs computation on elliptic curve three times, including sending two messages and receiving two messages.

In Table **2**, we show the results of Complexity analysis after comparing with E-G Scheme, KEP/KDP [18], ECMQV and [19]. In E-G Scheme, each node selects some keys from key pool to construct its own key pool, and each key agreement between two nodes need k times verification computation. KDP and KEP are proposed in [18] that adopt AES-128bits Packet encryption technology, however, both of them require the brute force attack to retrieve the shared key from the received message, and the cost of Hash function is much higher. In [19], each node needs a Hash signature and encryption respective twice, however, the cost is too high. Protocol 1 in this paper, each node needs to store only its own private/public key and system key. Each key agreement is only to be calculated thrice. The cost of ECC is much lower than that of Hash and Tate pairing.

As seen from Table **2**, the complexity of Protocol 1 is lower than that of other schemes (shown in Table **2**), KEP/KDP adopt Hash to signature and authenticate, the complexity is higher than ECC. Though ECC is adopted in E-G, the complexity of E-G is much higher.

Table 1. Performance analysis.

Process	Computation	Communication
Key generation	$3e_1$	$2e_2 + 2e_3$
Key update	$3e_1$	$2e_2 + 2e_3$

Table 2. Complexity analysis.

Protocol	Computation Complexity	Communication Complexity	Storage Complexity
Protocol 1	o(3)	o(3)	o(2)
E-G	o(k)	o(k)	o(k)
KEP	o(L)	o(L)	o(2)
KDP	o(L)	o(L)	o(2)
ECMQV	o(5)	o(5)	o(2)
[19]	o(4)	o(4)	o(2)

CONCLUSION

On the basis of ECC, this paper proposes a WSN authenticated key agreement protocol. Compared with other cryptography system, ECC have advantage of lower complexity and higher security. For Protocol **1** we proposed better performance than Hash and Tate pairing. Security analysis shows that Protocol **1** can provide Known-key security, Forward secrecy, Key-compromise impersonation, Unknown key-share resilience, Key control forward/back security and PKG forward security.

As shown in the performance analysis, we can see that in Protocol **1** we need fewer resources and require fewer computation and storage. A comparison of E-G, KEP/KDP, ECMQV and Protocol **1** shows that it is more suitable for WSN.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

We wish to acknowledge China Academy of Engineering Physics, expansion funds (2012A0403021).

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor network: a survey," *Comput. Networks*, vol. 38, no. 4, pp. 393-422, 2002.

[2] A. Shamir, "Identity based cryptosystems and signatures schemes", In: *Proc. of the Adv. Cryptol.*, New York: Springer-Verlag, pp. 47-53, 1984.

[3] Y. Zhang, W. Liu, W. Lou, Y. Fang, "Location based compromise-toler ant security mechanisms for wireless sensor networks," *IEEE J. Selected Areas in Comm.*, vol. 24, no. 2, pp. 247-260, 2006.

[4] W. He, M. Du, P. Liu, Z. Chen, "Wireless AD-hoc network group key management scheme based on paillier homomorphic", *Comput. Sci.*, vol. 40, no. 10, pp. 41-47, Oct. 2 013.

[5] Y. Li, Y. Liu, D. Lin, "Secure group key transfer protocol against insider attack", *Comput. Eng. Appl.*, vol. 50, no. 6, pp. 68-71, Jun. 2004.

[6] D. Liu, P. Ning, W. Du, "Group-based key predistribution for wireless sensor networks", *ACM Trans. Sensor Network,* vol. 4, no. 2, pp. 1-20, 2008.

[7] Z. Yu, Y. Guan, "A key management scheme using deployment knowledge for wireless sensor networks", *IEEE Transac. Parallel Distribut. Syst.*, vol. 19, no. 10, pp. 1413-1420, 2008,

[8] N. Guan, A. Patel, A. Wander, H. Eberle, S.C. Shatz, "Comparing elliptic curve cryptography and RSA on 8-bits CPUS", In: *Proc. of 6th Int. Workshop Cryptograph. Hardware Embedded Systems*: Boston, USA, 2004, pp.119-132.

[9] N. Koblitz, "Elliptic curve cryptosystems" *Mathemat. Computat.*, vol. 48, pp. 203-209, 1987.

[10] V. Miller, "Uses of elliptic curves in crypto graphy", *Adv. Cryptol. CRYP YO'85. LNCS218, Springer-Verlag*, pp. 417-426, 1986.

[11] L. Law , A. Menezes, M. Qu, J. Solonas, S. Vanstone, "An efficient protocol for authenticated key agreement", *Desig. Cod. Cryptograp.*, vol. 28, pp. 119 -134, 2003.

[12] D. J. Malan, M. Welsh, M. D. Smith, "A Public key infrastructure for key distribution in tiny OS based on elliptic curve crypt ography", In: *Proceedings of 1st IEEE Int. Conf. Sensor Ad Hoc Comm. Networks*, New York: 2004, pp. 71-79.

[13] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, P. Kruus, "TinyPK: Securing sensor networks with public key technology", In: *Proc. 2nd ACM Workshop Security Ad Hoc Sensor Networks*, New York: ACM Press, 2004, pp. 59-64.

[14] L. B. Oliveira, D. F. Aranha, E. Morais, F. Daguano, J. Lopez, R. Dahab, "TinyTate: computing the tate pairing in resource-constrained Sensor nodes" In: *6th IEEE Int. Sym. Network Comput. Appl. Cambridge*, MA: USA, 2007, pp. 318-323.

[15] H. Cheng, G. Yang, J. Wang, X. Huang, "An authenticated iden tity based key establishment and encryption scheme for wireless sensor networks", *J. China Univ. Posts Telecomm*. vol. 13, no. 2, pp. 23-29, 2006.

[16] D. Boneh, M. Franklin, Identity-based encryption from weil pairing[EB/OL]. (2008)[2010-06], http://eprint, iacr, urg/

[17] S. B. Wang, Z. F. Cao, X. L. Dong, "Provably secure identity-based authen ticated key agreement protocols in the standard model", *Chinese J. Comput.*, vol. 30, no. 10, vol. 1842-1854, 2007.

[18] C. T. Han, J. W. Wong, J. Zhou, *Implementiation and Perfo rmance Analysis for Key Divergent and Evolution Protocols in Wireless Sensor Network*, MobiQuitous, Dublin, Ireland, July 21-25, 2008.

[19] H. K. Kalita, A. Kar, "Key management in secure self organized wireless sensor network: A New Approach", *Int. Conf. Workshop Emerg. Trends Technol.*: Mumbai, India, 2011.

Received: September 22, 2014 Revised: November 30, 2014 Accepted: December 02, 2014