A SECURE ENCRYPTION LOGIC FOR COMMUNICATION IN WIRELESS SENSOR NETWORKS

Shanta Mandal[1] and Rituparna Chaki[2]

[1] Department of Computer Science and Engineering, West Bengal University of Technology, Salt Lake, Kolkata, India
shanta.mandal.ghosh@gmail.com
[2] Department of Computer Science and Engineering, West Bengal University of Technology, Salt Lake, Kolkata, India
rituchaki@gmail.com

ABSTRACT

This paper presents an encryption scheme suitable for direct diffusion protocols. We have calculated computational and communication overheads in terms of energy consumption using Directed Diffusion protocol. Public-key cryptography has been observed to suffer from high computational complexity and overhead. The symmetric-key schemes can be utilized more efficiently in order to provide more security. The proposed scheme overcomes the limitations of public-key and symmetric-key protocols for wireless sensor networks in respect of low energy consumption. The symmetric-key function is used to guarantee secure communications between the nodes in a network while the public-key function is used to guarantee a secure data delivery between the source to sink. This scheme provides mix of symmetric-key and public-key cryptography functions using the pre-distributed keys to implement data confidentiality service and Special attention for data authenticity.

KEYWORDS

Public Key Cryptography, Symmetric Key Cryptography, Secure hashing Algorithm, Data centric Protocol, Direct Diffusion Protocol.

1. INTRODUCTION

Wireless sensor networks (WSN) are widely used in different fields. The sensor nodes, which are intended to be physically small and inexpensive, are equipped with one or more sensors, a short-range radio transceiver, a small micro-controller, and a power supply. WSN consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location. Energy awareness is critical, especially in situations where it is not possible to replace sensor node batteries so it is essential design issue in wireless sensor networks. Most sensor network applications aim at monitoring or detection of phenomena likes office building environment control, wildlife habitat monitoring, and forest fire detection. Security is a key consideration when deploying Wireless Sensor Networks. Security is a well-established field for general-purpose computing where security mechanisms address computing services (e.g. authentication, intrusion detection, etc.) and Provide secure transaction. Since the battery life confines the lifetime of a sensor node, power consumption is normally set as the first priority in developing security solutions. Sensor networks are deployed in a hostile environment, security be-

DOI:10.5121/ijcis.2012.2310

comes extremely important as these networks are prone to different types of malicious attacks. To provide security, communication transactions should be encrypted and authenticated. Symmetric key scheme is more appropriate cryptography (SKC) for wireless sensor networks due to its low energy consumption and simple hardware requirements, but most of them cannot provide sufficient security level (e.g. integrity, confidentiality, and authentication) as public key approach (PKC) does.

Cryptographic primitives are the basis of security solutions and the most frequently executed security operations in sensor networks. Cryptography is the art of achieving security by encoding messages to make them non-readable. Cryptography is the study of hiding information that enables you to store sensitive information and also transmit it across insecure networks but it cannot be read by anyone except the intended recipient. Symmetric algorithms, both parties share the same key for encryption and decryption. The most common types are i) Symmetric Key Cryptography and ii) Public Key Cryptography. A public key cryptography algorithm uses two different keys for encryption and decryption. The key used for decryption kept secret (Private) whereas the encryption key can be distributed openly (Public). Encryption algorithms and their use are essential part of the secure transmission of information. There are extensive studies on using symmetric-key cryptography to achieve various aspects of security in sensor networks [5], [12]. The symmetric key function is used to guarantee secure communications between in-network nodes while the public key function is used to guarantee a secure data delivery between the source node and the sink node.

This paper describes a new hybrid approach that combines the advantages of the well-known PKC and SKC schemes in wireless sensor networks with direct diffusion protocol. It is suitable for wireless sensor networks that incorporate data centric routing protocols. Symmetric-key and public-key both are used insecurity implementation. We have calculated energy consumption with respect to message size in the new scheme.

Rest of the paper is organized as follows: section 2 deals with the state of the art studies in this field, section 3 presents the proposed framework, section 4 includes the simulation results, followed by conclusion in section 5.

2. RELATED WORK

The main challenge in sensory networks is how to secure communications between sensor nodes and how to set up secret keys between communicating nodes. We have calculated the computational and communication overheads using Public and Private Key in terms of energy consumption in the new scheme using Directed Diffusion protocol that incorporate data centric routing protocols.

In Data-Centric routing, querying an attribute of the phenomenon is used rather than querying an individual node. It also used in-network aggregation of data to yield energy-efficient dissemination and also it is good scheme for minimizing communication overhead and energy consumption. In data-centric routing, the sink sends queries to certain regions and waits for data from the sensors located in the selected regions. Data centric routing has proven to be a good scheme for minimizing communication overhead and energy consumption by using in-network aggregation.
Directed Diffusion [17] is a data-centric routing algorithm for sensor networks. Its key features are named attribute attribute-value pairs and path reinforcement [9], [13]. Once sources detect a matching target and send low-rate events, possibly along multiple paths, towards the sink. After the sink starts receiving these low data rate events, it reinforces one particular neighbour to find the higher quality events. So the sink re-sends the original interest message. These interest messages are flooding through the network and are added to each node's interest cache. Each interest

record in has one or more gradients correspond to neighbour nodes that transmitted the interest stored in cache. When the neighbouring node receives this interest, it notices that it has already gradient towards this neighbour. The node must also reinforce at least one neighbour if the data rate is higher than any existing gradient. The sink node finds the shortest path by sending an interest with a higher data rate along that path. Slower data paths may be sent negative reinforcement, i.e. interest messages with a slow data rate to save network bandwidth. The proposed scheme is suitable for wireless sensor networks that in data centric routing protocols. We have calculated the computational and communication overheads in terms of energy consumption with different message size in the new scheme using Directed Diffusion protocol. In this section, explain how different security schemes can be implemented in Direct Diffusion (DD) protocol. In DD protocol an interest travels between three different nodes the sink node, intermediate node, and source node. Therefore, the scheme shows how much energy is consumed to run such implementation within the node with different message size. Directed Diffusion routing protocol has been developed in data-centric routing [4], [7]. The DD protocol has several advantages. First, there is no need for a node to have a global or a local address since all communications occurs between neighboring nodes. Second, it is highly energy efficient since the node does not have to maintain global information about network topology. Finally, individual nodes can do aggregation and caching, in addition to sensing. We assume that a node uses the first radio model for sending and receiving data [2], [3]. This problem is known as the key agreement problem which has been handled via two security mechanisms: Public Key Cryptography (PKC) and Symmetric Key Cryptography (SKC). Mohammad AL-Rousan, A. Rjoub and Ahmad Baset used Directed Diffusion (DD) protocol that uses Elliptic Curve Cryptography (ECC) public key and RC5 symmetric key. But the novel proposed scheme uses ECC public key and scalable encryption algorithm (SEA) symmetric key and it is most suitable for wireless sensor networks.

Data aggregation [19] is the combination of data from different sources, and can be implemented in a number of ways. Aggregation functions are max, min, or any other function with multiple inputs. For our modelling purposes the aggregation function is such that each intermediate node in the routing transmits a single aggregate packet even if it receives multiple input packets. The idea is to combine the data coming from different sources are eliminating redundancy, minimizing the number of transmissions and saving energy. This paradigm shifts the focus on data-centric approach (finding routes from multiple sources to a single destination that allows in-network consolidation of redundant data).

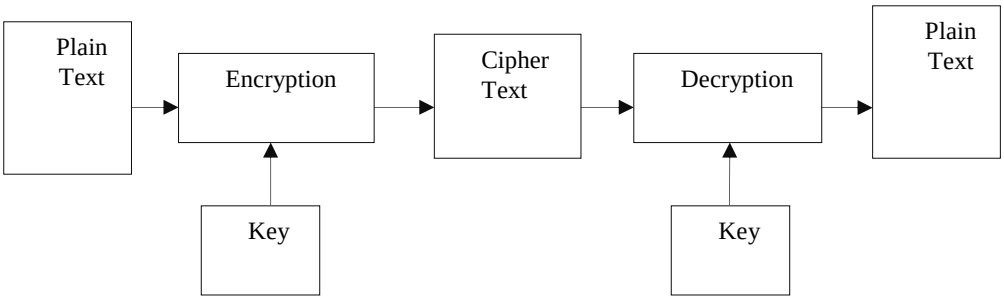

Figure 1. Basic Cryptographic Approach

Cryptography can be defined as conversion of data plaintext (ordinary text) into cipher text (known as encryption), then back again (known as decryption) into plain text. Due to the resource constraints, security and cryptography is an open issue for WSNs. If we consider both symmetric and asymmetric key management systems we can see that the implementation of both these systems is not practical for WSNs. A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination

with a key, a word, number, or phrase to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. "Cryptography" derives from the Greek word kryptons, meaning "hidden".

Symmetric-key Cryptography (SKC): In a symmetric-key algorithm both parties use the same key for encryption and decryption (DES, AES, RC5, SEA).

Public-key Cryptography (PKC): Asymmetric cryptography algorithms use different keys for encryption and decryption. Each node in the network has a pair of keys, the private key and the public key (RSA, Diffie-Hellman, ECC).

PKC is preferred for security purpose as it provides security services for the system under consideration including confidentiality, integrity, authentication, and non repudiation [14]. For network deployment to implement a secure Directed Diffusion using the hybrid security scheme it Store Public key, Symmetric key, and hash function codes in each node and also each node, select and save a randomly private key and keep the associated public key at the sink. It Save a public key of the sink at each node and the same common symmetric key in all sensor nodes. The drawback of PKC is that it suffers from high computational complexity and overhead so PKC schemes must be improved to their high complexity and high memory overheads. ECC [8] requires lower key size than RSA to achieve the same security level so ECC is more efficient than RSA [1] in terms of memory requirements. So the author uses ECC as a public key cryptography. The experimental result of executing the ECC with 160-bit key size and 1024-bit message size [10] shows that the execution time of the ECC on 8-bit ATMEL microprocessor with 8 MHz clock rate is 0.81s. The main idea In SKC techniques are that it must be utilized more efficiently in order to provide more security satisfaction and the secret keys are pre-distributed among sensors before their deployment [11]. The paper uses RC5 as a symmetric key, which has substantial overhead associated with its implementation. The symmetric key encryption does not guarantee authenticity or the integrity for that reason we uses secure hashing algorithm [6]. Confidentiality [16] means data remains private. Data integrity [16] is to ensure data is protected from accidental or deliberate (malicious) modification. Integrity is usually provided by message authentication code or hashes which is fixed length numeric value derived from a sequence of data. When the data sent through insecure channels Hash values are used to verify the integrity. The hash value of received data is compared to the hash value of the data as it was sent to determine if the data was altered. Authentication [16] is to assure that data originates from a particular party.

3. PROPOSED WORK

In this section we elaborate the proposed schema used for sensor networks. The study of previous works show that the use of RC5 often leads to high energy consumption and substantial overhead associated with its implementation. In this paper, a novel method for key generation using Scalable Encryption Algorithm (SEA) is proposed in order to reduce the energy consumption of the network. The symmetric key encryption does not guarantee authenticity or the integrity. The secure hash function is used for this purpose, albeit with additional (h) bits to be sent along with the original data packet and here we proposed to use SEA [20] as a symmetric key.

The proposed scheme uses ECC public key and SEA symmetric key and is suitable for wireless sensor networks that incorporate data centric routing protocols. In DD protocol an interest travels between three different types of nodes; the sink node, the intermediate node(s), and the source node. Therefore, we show how each of these node implements the security schemes under consideration and how much energy is consumed to run such implementation within the node. The scheme involves three phase,

(i) source_node,
(ii) intermediate_node
(iii) sink_node.

3.1. Algorithm

Data packet Encryption and Decryption by the Source, intermediate and sink node.

M bit data packet encrypted by the symmetric and public key using hash (h) function.
Then m+h bit encrypted message send from source node to sink or intermediate node.

If m+h bit data packet was received by the sink node.
{
else
m+h bit message received by the intermediate node.
The packet is decrypted by using public key and symmetric key with hash function.
The decrypted message checks the data aggregations.
Then the data packet was encrypted by using both public key and symmetric key with hash function.
The encrypted packet sent to the next node.
If the next node is not the sink node, then repeat the above process
}
The sink node decrypts the received packet using public and symmetric keys with hash function.

3.2. Logic Description

3.2.1. Phase (i) Source_node

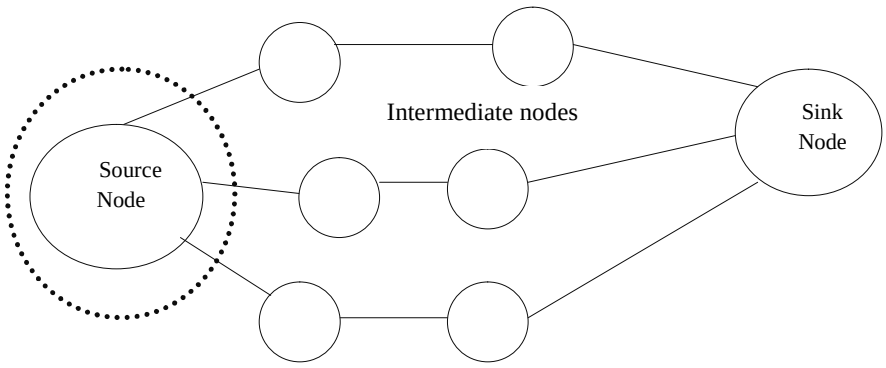

Figure 2. source_node centric graph

This is the case when the data is encrypted/decrypted by the source node itself. Data is encrypted by using both the symmetric and public key techniques. To guarantee the authenticity and integrity symmetric key encryption is coupled with hash function. The final encrypted message m associated with additional h bits. Finally m+h bit data packet is sent to intermediate node.

3.2.2. Phase (ii) Intermediate_node

This part deals with the steps executed by each intermediate node after receiving the encrypted. Our proposed scheme use direct diffusion protocol, a well known data centric routing protocol to yield energy efficient dissemination in-network aggregation.

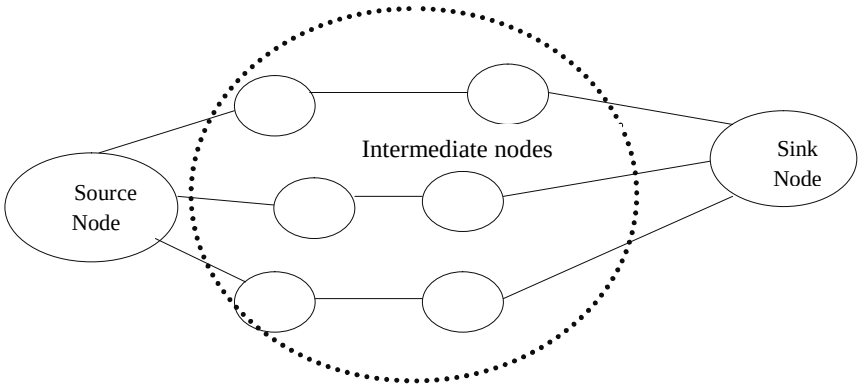

Figure 3. intermidiate_node centric graph

The copies of similar data are replaced by a single message it is known as data aggregation. It is important feature of DD protocol. For intermediate nodes, each node does not need to encrypt the part of the packet that is encrypted by the source/sink node using the public key, it rather needs to decrypt and encrypt the aggregation data. This is done by using the scalable encryption algorithm (SEA) and SHA. Suppose there are two messages M1 and M2, such that M1=M2 encrypted and decrypted by the same key. So the node will only check if the encrypted data already exists in the data cache. The proposed techniques first decrypt the message and checks for its existence in cache. The message is then encrypted using hashing algorithm and scalable encryption algorithm. The encrypted message is then sent to next step mean phase three. We would to emphasis here that not all fields in the packets (interests and replies) are needed for aggregation at intermediate nodes, while the sink and the source must see the whole packet.

3.2.3. Phase (iii) Sink_node

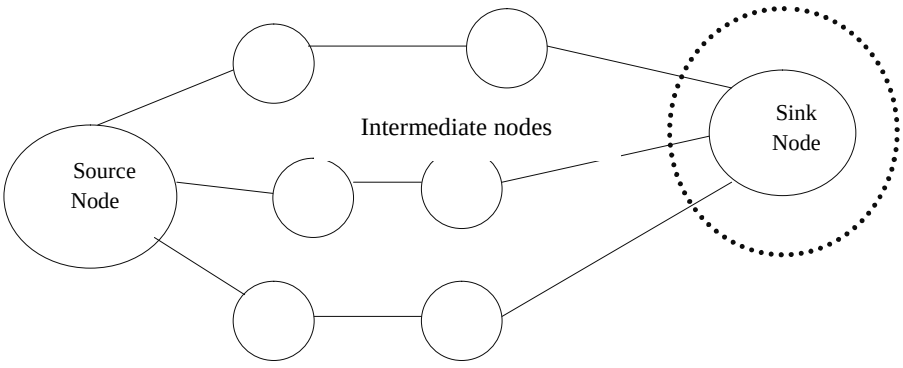

Figure 4. sink_node centric graph

This section describes the steps executed by sink node after receiving the encrypted message. The sink node decrypts the received data using the ECC and SEA algorithm.

In our paper[18] already show and compare the energy consumptions at the sink, source, and intermediate node for all security schemes (SEA, RC5, ECC) under consideration. The proposed paper shows that the energy consumption at the source, sink and intermediate nodes with respect to the different message size.

4. RESULT DISCUSSION

This section presents a comparative analysis of the proposed technique against the techniques as presented in [15]. It is assumed that the proposed scheme is executed on Atmega 128 16MHz 8-bit architecture AVR instruction set. Now analyze the energy consumption of the symmetric key for encryption/decryption process. The network size is taken as n= 10. In our discussion we show and compare the energy consumptions at the sink, source, and intermediate with different message size (m). In the proposed scheme used 1024, 2048, 4096, 8192, 16384 message size.

Figure 5 compares the energy consumed by source node in the hybrid scheme. The energy consumption by source node reduces with respect to the schemes proposed in [15]. The key idea behind the hybrid scheme is that it uses PKC and SKC in the encryption/decryption process. The reason for improvement is attributed to the fact that RC5 has been replaced by SEA. The key-size generated by using RC5 tends to be larger than that generated by SEA. Thus the energy consumed in generating the encryption for RC5 is more than that needed for SEA.

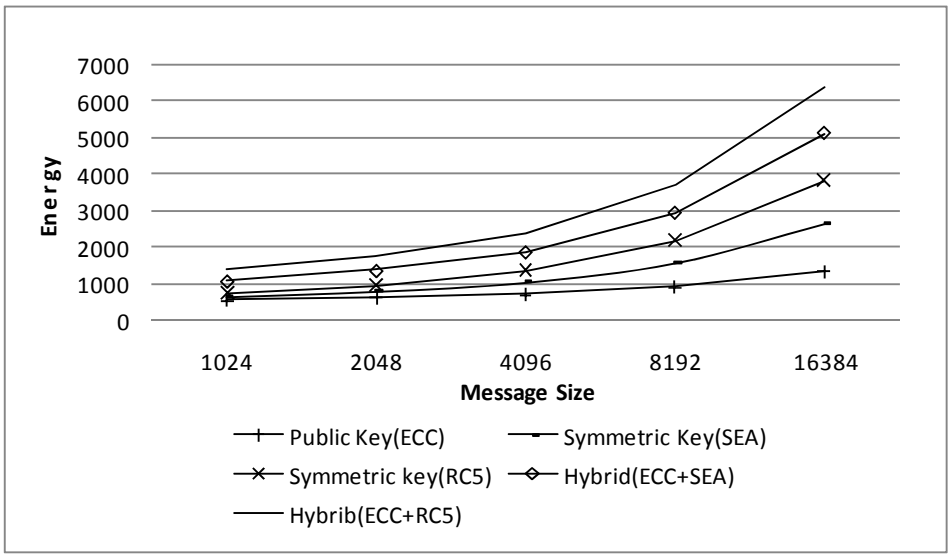

Figure 5. Energy Consumption at Source Node

Figure 6 compares the energy consumed by the intermediate node in the hybrid scheme. The key idea behind the hybrid scheme is that it uses PKC and SKC in the encryption/decryption process. The energy consumption by intermediate node is less than the schemes proposed in [15]. The proposed hybrid security scheme suggests that a symmetric key algorithm should be used by the intermediate nodes to encrypt/decrypt the aggregate data portion, while the required data portion is encrypted/decrypted using a public key algorithm.

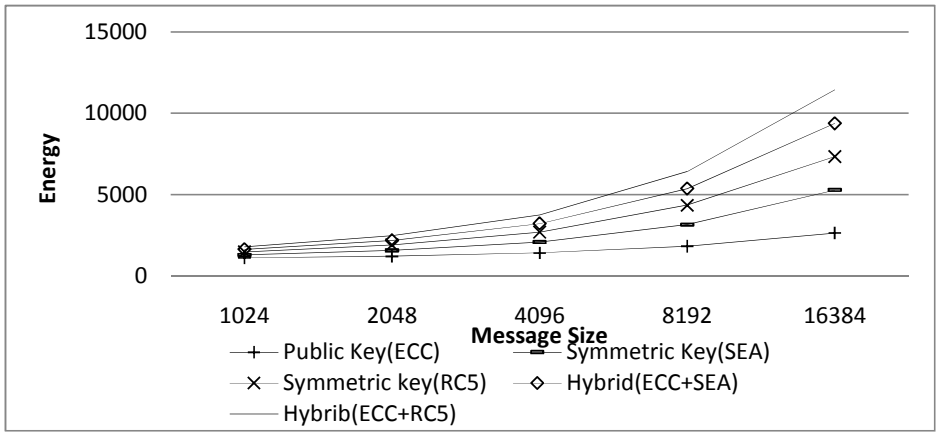

Figure 6. Energy Consumption at Intermediate Nodes

Figure 7 compares the energy consumed by the sink node in the hybrid scheme. The key idea behind the hybrid scheme is that it uses PKC and SKC in the encryption/decryption process. The energy consumption by sink node reduces with respect to the schemes proposed in [15]. The reason for improvement is attributed to the fact that RC5 has been replaced by SEA. The key-size generated by using RC5 tends to be larger than that generated by SEA. Thus the energy consumed in generating encryption and decryption key for RC5 is more than that needed for SEA.

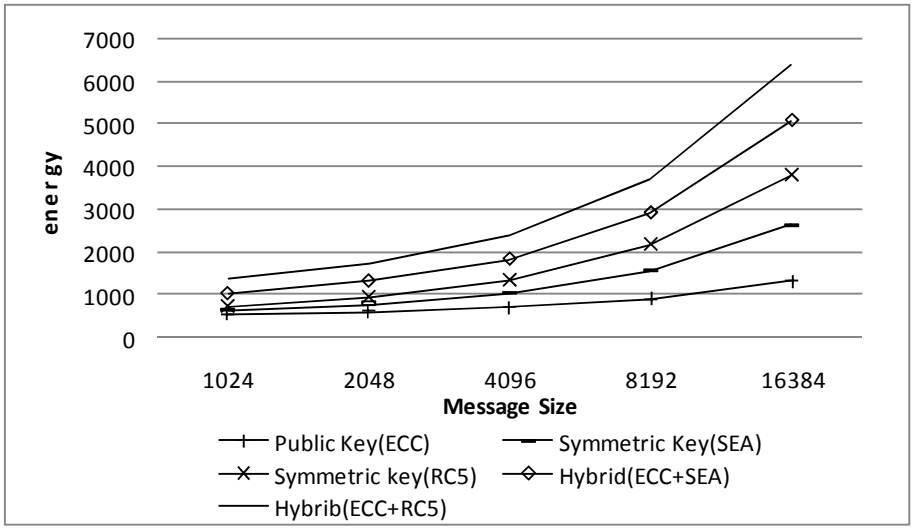

Figure 7. Energy Consumption at Sink Node

Figure 8 shows the average energy consumption of the overall node. The approach shows that if we are using SEA instead of RC5 [15] (Rivest Cipher 5) then the energy consumption will be reduced a lot. The key-size generated by using RC5 tends to be larger than that generated by SEA. Thus the energy consumed in generating the encryption and decryption key for RC5 is more than that needed for SEA.

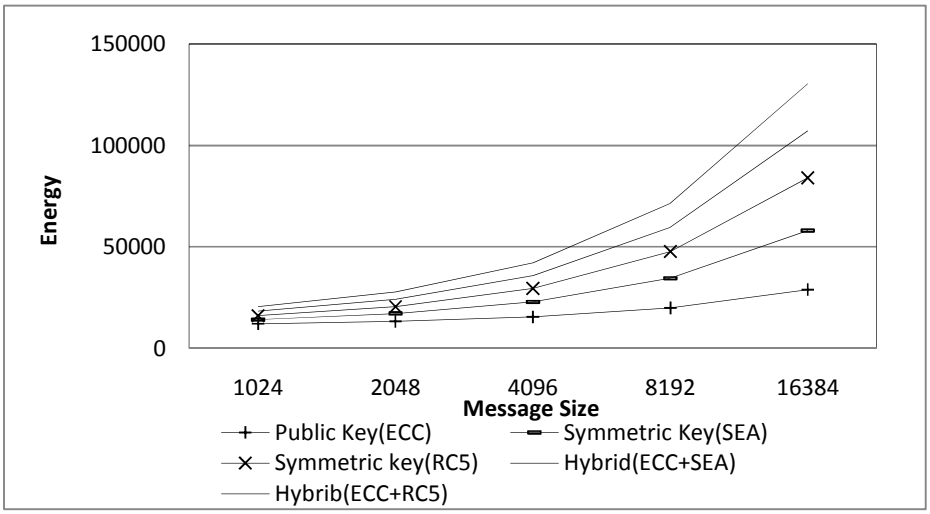

Figure 8. Overall Energy Consumption

5. CONCLUSION

This paper proposes a technique for minimizing the energy consumption in encrypting data packets. The scheme is suitable for data centric routing protocol. The key idea behind the scheme is that it uses PKC and SKC in the encryption/decryption process. SKC schemes can be utilized more efficiently in order to provide more security when PKC suffers from high computational complexity and overhead. The proposed security scheme overcomes the limitations of both public-key and symmetric-key protocols. It uses secure hashing algorithm and this will incur additional (h) bits to be sent along with the original data packet guarantee for authenticity or the integrity. Here we are using Scalable Encryption algorithm instead of RC5. Public key function is used to guarantee a secure data delivery between the source to sink node while the symmetric key function is used to guarantee secure communications between the nodes in a network.

ACKNOWLEDGEMENT

This project has been partially funded by “Advanced Technology Cell” (Joint Programme between DRDL and Jadavpur University) under “ACT/Student-Project/2011-12/22” scheme. I take this opportunity to thank the entire team of “Advanced Technology Cell” for their kind encouragement.

REFERENCES

[1] R.L. Rivest, A. Shamir & L.A. Adleman, (1998) “A method for obtaining digital signatures and public-key crypto systems”, Communications of the ACM 21(2), pp120–126.

[2] Heinzelman W., Kulik J. & BalakrishnanH, (1999) “Adaptive Protocols for Information Dissemination in Wireless Sensor Networks”, In Proceedings of the 5thACM/IEEE Mobicom, pp174–185.

[3] Heinzelman W, Chandrakasan A, & Balakrishnan H, (2000) “Energy-Efficient Communication Protocol for Wireless Micro sensor Networks”, In Proceedings of the 33rd Annual Hawaii Interna-tional Conference on System Sciences (HICSS 33), pp1-10.

[4] If. Akyildiz, W. Su, Y. Sankarasubramaniam & E. Cayirci, (2001) “Wireless sensor networks”, a survey. Computer Networks 38(4), pp393-402.

[5] H. Chan, A. Perrig & D. Song, (2003) “Random key pre distribution schemes for sensor net-works”, In Proceedings of the IEEE Symposium on Research in Security and Privacy, pp197–213.

[6] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller & M. Sichitiu, (2003) "Analyzing and modeling encryption overhead for sensor network nodes", In Proceedings of WSNA '03, pp151-159.
[7] R. Di Pietro, L. V. Mancini, Y. W. Law, S. Etalle & P. Havinga, (2003) "LKHW, A directed diffusion-based secure multicast scheme for wireless sensor networks", In Proceedings of the First International Workshop on Wireless Security and Privacy (WiSPr'03), pp397-406.
[8] G. Gaubatz, J. Kaps, B. Sunar, (2004) "Public keys cryptography in sensor networks", In Proceedings of the 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS).
[9] J. N. Al-Karaki &A. E. Kamal, (2004) "Routing Techniques in Wireless Sensor Networks: A Survey," IEEE Wireless Communication, Vol. 11, pp6-28.
[10] N. Gura, A. Patel, A. Wander, H. Eberle & S. Shantz, (2004) "Comparing elliptic curve crypto-graphy and RSA on 8- bit CPUs", In Proceedings of the 6th International Workshop on Crypto-graphic Hardware and Embedded Systems, Cambridge, MA, pp119-132.
[11] J. Lee & D. R. Stinson, (2005) "Deterministic key pre distribution schemes for distributed sensor networks", In Proceedings of the ACM Symposium on Applied Computing, vol. LNCS 3357, pp294-307.
[12] Y. Cheng & D.P. Agrawal, (2005) "Efficient pair wise key establishment and management in static wireless sensor networks", In Proceedings of the Second IEEE International Conference on Mobile ad hoc and Sensor Systems, Washington, DC.
[13] C. Intanagonwiwat, R. Govindan & D. Estrin, (2006) "Directed diffusion: A scalable and robust communication paradigm for sensor networks", in the Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'00), Boston, MA, pp56-67.
[14] Y. Law, J. Doumen & P. Hartel, (2006) "Survey and benchmark of Block Cipher for Wireless Sensor Neworks," ACM Transactions on Sensor Networks 2(1), pp65-93.
[15] Mohammad AL-Rousan, A. Rjoub & Ahmad Baset, (2009) "A Low-Energy Security Algorithm for Exchanging Information in Wireless Sensor Networks", Journal of Information Assurance and Security 4, pp 48-59.
[16] Ayushi, (2010) "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15.
[17] K.E.Kannammal, Dr.T.Purusothaman &K.E. Kannammal et. Al, (2010) "Evaluation of Directed Diffusion Protocol for Mobile Sensor Networks," International Journal of Engineering Science and Technology Vol. 2(6), 2272-2277.
[18] Shanta Mandal & Rituparna Chaki (2012) "A Novel power balanced encryption scheme for se-cure information exchange in Wireless Sensor Network" Advances in Intelligent Systems and Computing, 1, Volume 176, Advances in Computing and Information Technology, pp 263-271.
[19] Bhaskar Krishnamachari, Deborah Estrin, & Stephen Wicker, "Modelling Data-Centric Routing in Wireless Sensor Networks", Computer Engineering Technical Report CENG 02-14.
[20] Francois-Xavier Standaert1, Gilles Piret1, Neil Gershenfeld & Jean-Jacques Quisquater, "SEA a Scalable Encryption Algorithm for Small Embedded Applications".

Authors

Shanta Mandal is Pursuing M-tech in software engineering department of Computer Science and Engineering from West Bengal University Of Technology. Her area of Research area is Wireless Sensor Network.

Rituparna Chaki is an Associate Professor in the Department of Computer Science & Engineering, West Bengal University of Technology, Kolkata, India, since 2005. She received her Ph.D. in 2002 from Jadavpur University, India. The primary area of research interest for Dr. Chaki is Wireless Mobile Ad hoc Networks and Data Mining. She has also served as a Systems Manager for Joint Plant Committee, Government of India for several years before she switched to Academia. Dr. Chaki also serves as a visiting faculty member in other leading Universities including Jadavpur University. Dr. Chaki has about 45 referred international publications to her credit.