ENERGY-EFFICIENT AND SECURE PATTERNBASED DATA AGGREGATION FOR WIRELESS SENSOR NETWORKS

Dr. Bhupinder Singh dhaliwal, Vivek Soi

Abstract— **This paper studies the challenging problem of energy minimization for data gathering over a multiple-sources single-sink communication substrate in wireless sensor networks by exploring the energy-latency tradeoffs using rate adaptation techniques. We consider a real-time scenario for mission-critical applications, where the data gathering must be performed within a specified latency constraint. We first propose an offline numerical optimization algorithm with performance analysis for a special case with a complete binary data gathering tree. Then, by discretizing the transmission time, we present a simple, distributed on-line protocol that relies only on the local information available at each sensor node. Extensive simulations were conducted for both long and short-range communication scenarios using two different source placement models. We used the baseline of transmitting all packets at the highest speed and shutting down the radios afterwards. Our simulation results show that compared with this baseline, up to 90% energy savings can be achieved by our techniques (both off-line and on-line), under different settings of several key system parameters.**

Index Terms—**About four key words or phrases in alphabetical order, separated by commas.**

I. INTRODUCTION

ENERGY-EFFICIENCY is a key concern in wireless sensor networks (WSNs) [2]. One useful mechanism for energy-efficient communication is to explore the energylatency tradeoffs by adjusting the transmission time [3]. An important observation is that in many channel coding schemes, the transmission energy can be significantly reduced by lowering transmission power and increasing the duration of transmission [3]. Rate adaptation techniques (e.g., modulation scaling [4]) have been proposed for implementing such tradeoffs. In this paper, we exploit the energy-latency tradeoffs in the context of data gathering in WSNs. Typical communication patterns in data gathering involve multiple data sources and one data sink, forming a reverse-multicast structure, called the data gathering tree [5]. Data aggregation along such a tree [5] is particularly useful in eliminating data redundancy and reducing the communication load. We consider a realtime mission-critical scenario where the raw data gathered from the source nodes must be aggregated and transmitted to the sink within a specified latency constraint. Our objective is to minimize the overall energy cost of the sensor nodes in the data gathering tree subject to the latency constraint. Although our problem is formulated as a convex programming problem which is solvable in polynomial time by using general optimization tools, we propose more a time-efficient algorithm in this paper by exploiting special properties of the problem. Such properties include the convexity of the energy function of wireless communication and the tree structure of the underlying communication substrate. It is important to evaluate the usefulness of the latencyenergy tradeoffs by examining the sources of latency and energy costs for data gathering in WSNs. We assume a low-duty cycle WSN with sleep scheduling so that nodes are completely shut down in idle state. In such a system, besides the time cost for packet transmission, the latency for data gathering can be further decomposed into queuing delay, channel access delay, re-transmission delay, and the delay for waking up sleeping nodes. We argue that under several reasonable assumptions, the packet transmission delay is significant and worth trading for energy. In the following paragraph, we explain our argument in detail. First, due to the application-specific design of WSNs, most traffic throughout the network is due to transporting the gathered data to the base station. It is also anticipated that many applications for WSNs require transmission of tens to hundreds of bytes per second [6]. In such a lighttraffic scenario, queuing delay is not as a major concern as it is in traditional wireless ad hoc networks. Second, we assume the availability of a collision-free medium access control (MAC) protocol (e.g., using multi-packet reception (MPR) techniques [7], [8]), so that channel access delay due to collision detection and avoidance is negligible. However, our techniques are not directly applicable to TDMA-based protocols, due to the extra waiting time for transmission slots, or to contention-based MAC protocols, due to the latency caused by packet collisions. Third, the number of expected re-transmissions is actually a function of the Bit Error Rate at the receiving node, which in turn determines the energylatency tradeoffs for packet transmission (see Section III-C for details). Therefore, it is convenient to explicitly incorporate the tradeoffs between expected number of re-transmissions and energy into our work. Fourth, we assume that a full duty cycle, ultra-low power wakeup radio [9] is available for each sensor node. Thus, sleeping sensor nodes can be woken up for packet transmission with almost no delay and energy penalties. Also, the typical startup time for sensor nodes is around 100 μSec [6], while the time for transmitting a packet of 200 bytes using 1 Mbps is 200 μSec. Based on the above observations, the time for packet transmission in light-traffic WSN applications constitutes a significant portion of the overall delay. Since we

Manuscript received April 23, 2015
Dr. Bhupinder Singh dhaliwal, Guru Kashi University
Vivek Soi, Guru Kashi University

assume that sensor nodes are completely shut down in idle state, the main source of energy cost is due to packet transmission for data gathering. It is therefore crucial to explore the energy-latency tradeoffs of packet transmission in such a context. Technical Approach Overview: We first present an off-line numerical optimization algorithm, where the structure of the data gathering tree and the energy characteristics of all sensor nodes are known a priori. We also analyze the performance of our algorithm for a special case over a complete binary data gathering tree. We then approximate the transmission time using a set of discrete values and describe a simple, localized on-line protocol. The key idea is to iteratively identify the sensor node with the highest energy gradient (to be defined later) in the tree and reduce its energy cost when allowed by the latency constraint. In this protocol, each sensor node only needs to perform simple operation based on its local information and the piggybacked information from data messages. Finally, we evaluate the performance of our techniques through extensive simulations. The simulations were conducted for both long and short-range communications.

II. RELATED WORK

2.1 (Subasree) Security Protocol Architecture [14]

This protocol is shown in Fig. 2. The given plain text can be encrypted with the help of ECC and the derived cipher text can be communicated to the destination through any secured channel. Simultaneously, the Hash value is calculated through MD5 for the same plain text, which already has been converted into the cipher text by ECC. This Hash value has been encrypted with DUAL RSA and the encrypted message of this Hash value also sent to the destination.

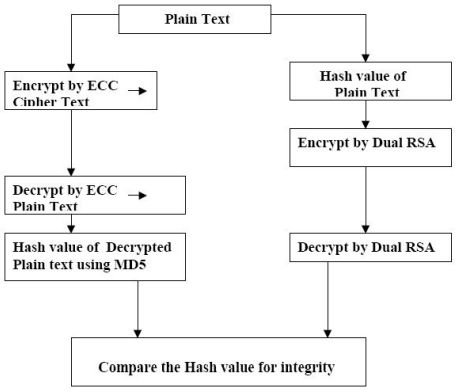

Fig. 2: (Subasree) Security Protocol Architecture [14]

there are two disadvantages. First, the message is encrypted by Asymmetric Encryption Algorithms (ECC and DUAL RSA Public key encryptions) that are slow compared to symmetric encryption. Second,if an attacker determines a person's private key, his or her entire messages can be read.

2.2 (Kumar) Security Protocol Architecture [15]

The protocol architecture is shown in Fig. 3. The given plain text is encrypted first with AES algorithm and then with ECC algorithm. The

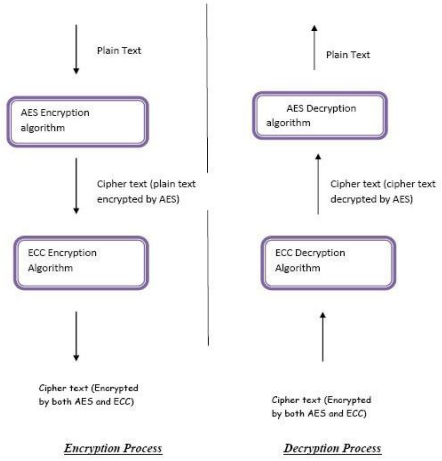

Fig. 3: (Kumar) Hybrid Protocol Architecture [15]

Hash value of this encrypted cipher text is taken through the MD5 algorithm. On the other side, the Hash value is first evaluated and integrated. Thereafter, the decryption of cipher text is done by AES and ECC decryption algorithms. Hence, the plaintext can be derived. The (Kumar) Security Protocol is a combination of both the Symmetric and Asymmetric Cryptographic Techniques. However, the execution time of this protocol is long because the plaintext is encrypted sequentially by both AES and ECC.

2.3 (Kady) Security Protocol Architecture [16]

The protocol architecture is shown in Fig. 4. The plaintext is divided into n blocks Bi. Each block consists of 128 bits. Then, it is divided into two parts p1 blocks, and P2 blocks. The first n/2 blocks are encrypted using (AES and ECC) . In parallel, the remaining n/2 blocks are encrypted using XOR-DUAL RSA algorithm. Then hashing each two half using MD5. In the Decryption Phase:The decryption phase the cipher text is divided into n blocks each block consists of 128 bits, Then it will divided into two parts ci blocks and Ci blocks.Hashing is used to identify whether the source node receive the same cipher text or not. In the case of the hash values are the same at the source and sink nodes, the first n/2 blocks are decrypted using AES and ECC algorithms .The remaining n/2 blocks are decrypted using XNOR-DUAL RSA algorithm.

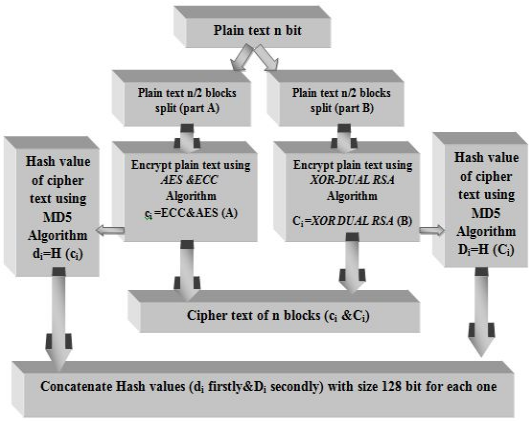

Fig. 3: (Kumar) Hybrid Protocol Architecture [15]

2.4 (Zhu) Security Protocol Architecture [17]

This protocol is shown in the Fig. 5. The plaintext is encrypted with Symmetric cipher algorithm, and the key and digital signature belonged to the Symmetric encryption algorithm are encrypted with Asymmetric key algorithm. The sender encrypts the plaintext P with the key KAES belonged to the AES algorithm. To ensure the security of the cipher algorithm and simplify the key management, the sender uses the key KAES only once. The receiver obtains the original information P after signature verification. The main disadvantage of this protocol, this protocol suffers from low security level since that the message is encrypted in a single phase which leads to less complexity.

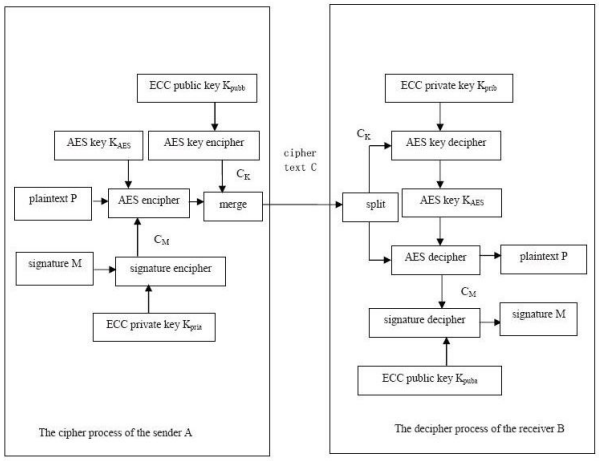

Fig. 5: (Zhu) Hybrid Protocol Architecture [17]

III. INFERENCES DRAWN OUT OF LITERATURE REVIEW

Following inferences are drawn out of literature review:

ECC- Elliptic Curve Cryptography provides great solution for security and authorization in the sensor network. Prime factors are strong case of security implemented in Sensor communication. Asymmetric key distribution will works for authorization.

Cluster Head Selection of cluster head is very important for implementation of security in sensor network. Moreover cluster selection for cluster head is also an issue that needs to take care.Privacy preservation is very much required in case user and owners are different entities and to make better communication and better upgrades, privacy needs to separately considered as focused part.

IV. PROBLEM DEFINATION

A secure Asymmetric key distribution scheme has been proposed for wireless sensor networks for reprogramming the software for upgrade and change in functionalities for sensor. After deployment of nodes, it provides sensors with predefined asymmetric keys which will be used for authorization of the users which can alter the reprogramming functionalities.Cluster head selection is based on the higher residual energy of the node and to avoid cluster head participation in two clusters, receives signal strength identifier is used. In some applications, the network owner and users are different entities. A user may want to hide his/her reprogramming privacy from anyone else including the network owner. In our experimentation, we will study how to support user privacy preservation in distributed reprogramming.

V. OBJECTIVES

The overall objective of any upgrade is to increase the working efficiency of the network but this research is focused on security. In the light of the problem stated above my objective is as given below: To improve the Privacy preservation in between owner and various users.To provide good authorized mechanism for users so that network can't be harm by unauthorized users and moreover privileges of the users can also be authorized.

VI. METHODOLOGY

Our experimentation will start with briefing knowledge about sensor network and the basic implementation of sensor network in OPNET 14.5 Modeler Simulator. Sensor field will be used as logical area with various sensor nodes and Single sink. We start our proceeding with pre deployment of sensor nodes and continue with implementation of traffic on sensor network. After this process we will distribute the pre defined asymmetric keys to all sensors. This key distribution will provide public encryption to the deployed network.

Next step will be of selection of cluster head selection will be done on the bases of total energy depleted by the sensor. Sensor with more energy remaining will become the cluster head. Energy will also be measured and must be more than threshold energy level. For the complete segregation of the users, we will use MD5 algorithm at login of the query initiation process which will be processed for ECC encryption further.

.

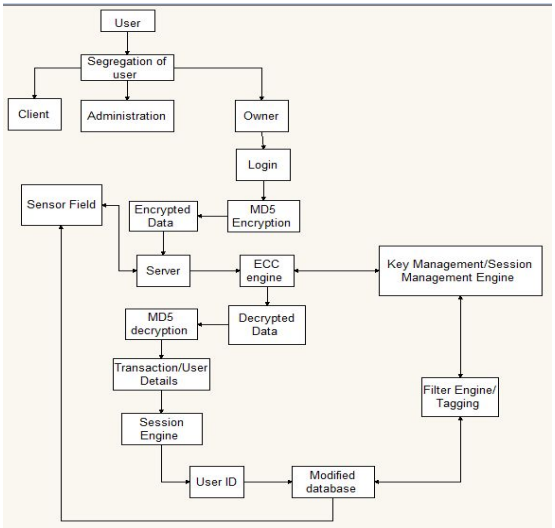

Figure 1.5: Detailed view of proposed work

Next step will be providing public key security to the sensor network. User will store the elliptic curved Integrated Encryption for providing strong security to sensor network. Only authorized users will be allowed to update the system reprogramming and with according to privileges carried by user, system upgrade options will be provided. User privilege and identity will be checked with signature of the message.

For managing privacy preservation between owner and other users we will introduce the different session keys for owner and users so that both can have different views of network and can also preserve their privacy from each other. The queries which need to modify will processed with tagging and specific keys with tagging will be assigned to them for the privacy preservation of the system with admin users.

CONCLUSION

Hence by modifying the images of sensor, we can enhance the performance and progress of sensor network. Elliptic curve encryption is the great support for encrypting various methods and Privacy preservation can be fulfill by session key generation. This scheme can give rise to a agile network management.

REFERENCES

[1] Daojing He, Chun Chen, " SDRP: A Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks", IEEE Transactions On Industrial Electronics, Vol. 59, No. 11, pp. 12-16, November 2012.

[2] Shanta Mandal and Rituparna Chaki," A Secure Encryption Logic for Communication in Wireless Sensor Networks", International Journal on Cryptography and Information Security (IJCIS), Vol.2, No.3, pp. 78-82, September 2012.

[3] Amar Rasheed, " The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks", IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 5, May 2012.

[4] Donnie H. Kim, "Exploring Symmetric Cryptography for Secure Network Reprogramming", International conference on Information, Networking and Automation(ICINA),Kunming, IEEE, pp. 215-218, 2010.

[5] Wassim Drira," A Hybrid Authentication and Key Establishment Scheme for WBAN", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Vol. 2, No.3, 2012.

[6] Shih-Hao Chang, Madjid Merabti, Hala Mokhtar, "A causal model method for fault diagnose in wireless sensor networks", 2010 10th IEEE International conference on Computer and Information Technology (CIT 2010), Bradford, IEEE, pp.155-162, 2010.

[7] Wei Ni, Wendong Xiao, Yue Khing Toh and Chen Khong Tham, "Fingerprint-MDS based algorithm for indoor wireless localization",21st Annual International symposium on personal, indoor and mobile radio communications, Istanbul, IEEE, pp.1972-1977, 2010.

[8] Daojing He, Chun Chen," Security Analysis and Improvement of a Secure and

[9] Distributed Reprogramming Protocol for Wireless Sensor Networks", IEEE Journal, Vol.5, Issue.8, pp. 19-22, September 2012.