IDKEYMAN: An Identity-Based Key Management Scheme for Wireless Ad Hoc Body Area Networks

Sriram Sankaran, Mohammad Iftekhar Husain, and Ramalingam Sridhar
Department of Computer Science and Engineering
University at Buffalo, The State University of New York, Buffalo, NY 14260

***Abstract*— Wireless Ad hoc Body Area Networks are primarily used in health-care applications for patient monitoring purposes. Publisher-Subscriber driven Body Area Networks enable publishers (medical sensors attached to patients) to disseminate medical data to numerous mobile heterogeneous subscribers (doctors or caregivers) through a subscription mechanism. Such an environment raises serious security concerns due to the privacy critical medical data coupled with the resource constraints of individual body sensors. To address this problem, we present an identity based key management scheme using Identity-Based Encryption (IBE). IBE facilitates faster key set-up in addition to being lightweight and energy-efficient. The proposed scheme uses IBE to set up pair-wise symmetric keys to preserve data confidentiality and integrity. Our prototype and evaluation of the proposed model validate the approach.**

I. INTRODUCTION

Wireless Sensor Networks have been applied in health-care environments termed Wireless Ad hoc Body Area Networks, also referred as Body Sensor Networks (BSN). BSN comprises of a group of sensors either attached to or implanted inside the human body. These sensors are often resource-constrained and facilitate remote monitoring of patients in hospital or emergency conditions thereby reducing health-care costs.

BSN differs from traditional sensor networks in several ways. The main difference lies in the privacy-critical medical data of patients. A BSN is a real-time system i.e. the collected data has to be readily available in real-time in the event of an emergency while failing to provide could result in severe life threatening problems. Also, lifetime of BSNs is critical with the pressing resource constraints of individual body sensors.

Security in BSN is of paramount importance due to the criticality of the medical data coupled with the resource constraints of individual body sensors requiring lightweight solutions. Security must be provided between patients and their authorized doctors/caregivers through key management solutions.

Ideally, security solutions proposed for BSN must satisfy the following security traits. For instance, medical data must be accessible only by corresponding patients and his/her authorized physicians thus ensuring confidentiality, as per HIPAA regulations [28]. To prevent medical data from getting into the hands of intruders/unauthorized people, medical data must be authenticated. With authentication in place, medical data must be integrity protected in order to prevent/detect data tampering. Finally, this data needs to be received and processed in real-time without incurring much delay.

In this paper, we consider publisher-subscriber driven body sensor networks, a key enabler for the design and development of CodeBlue system [2][3]. We propose a key management scheme, IDKEYMAN, for this communication model using Identity-Based Encryption (IBE). IBE facilitates faster key set up in addition to incurring low overhead. We use IBE to set up pair-wise symmetric keys between publishers and subscribers. Our scheme preserves the confidentiality, authenticity and integrity of safety critical medical data while also being energy-efficient. We tested our scheme on Prowler [12], a wireless sensor network simulator with Berkeley MICA mote [27] as the targeted platform.

II. RELATED WORK

Early research on key management for sensor networks focused on symmetric key based approaches since public key based approaches seemed to incur more overhead on the motes. Probabilistic key management was proposed by [4], where a pair of nodes wanting to communicate randomly picks keys from a key pool and communicates using the common shared key. Some variations were proposed to the above scheme termed as q-composite schemes and random pair-wise schemes in [7]. Q-composite scheme computes the pair-wise keys based on the hash of q-pre-distributed keys that the communicating entities share, thus decreasing the probability of node compromise. Random key improves on the q-composite scheme and further increases its resilience to node compromise by randomly picking its communicating entities, computing a random pair-wise key and attaching it to the key ring of the sensor's ID. Liu et al. [5] further study the probabilistic key approach proposed by [4] and construct a pool of several polynomials to generate pair-wise keys in contrast to key distribution based on a single polynomial to increase robustness towards node capture. Zhu et al. [8] combine the idea of probabilistic key approach and threshold key sharing to compute a pair-wise key between

communicating entities. Du et al. [6] improve Blom's scheme [20] and increase its network resilience by devising a pair-wise key pre-distribution scheme based on multiple key spaces in contrast to the single key space based approach proposed by [20]. While these schemes proposed for traditional sensor networks provide security support at the right time by resisting attacks, they may not readily satisfy the stringent resource constraints and real-time requirements of individual body sensors.

Recent research demonstrates public key methods such as Elliptic Curve Cryptography (ECC) to be feasible on the resource constrained motes [3]. Public key based approaches offer several advantages over symmetric key based approaches due to the ability to bootstrap security using a trusted authority. Our scheme offers even more advantages that it avoids the need for distributing public keys using trusted authority since identity is used as the public key. Furthermore, our scheme pre-deploys the motes with private keys making the private key generator unnecessary.

Elliptic curve based approaches have been proposed in the literature for security in sensor networks. Malasri et al. [1] devised an authentication scheme and an ECC based secure key exchange protocol for providing authentication of patients thereby ensuring message integrity and confidentiality. However, in contrast to their approach involving ECC, we have used identity based cryptographic primitives since it offers several advantages compared with ECC as mentioned above. In their scheme, Message Authenticated Code (MAC) was computed at every step of the key management process which makes it resource intensive and introduces delay in processing packets at the receiver. To minimize the processing delay, our approach involves computing the MAC only during data packet transmission phase.

Oliveira et al [9] proposed a security solution TinyTate for sensor networks based on IBE and claimed it to be feasible on the resource constrained motes. In contrast to their approach involving a traditional sensor network with a standard communication model, we consider body sensor networks that comply with Publisher-Subscriber model practically implemented in CodeBlue, one of the most complete frameworks in the healthcare context. Their scheme involves senders to broadcast their identities without any security support which allows adversaries to launch DoS attacks by broadcasting several fake identities draining the precious power of the resource constrained motes. To prevent DoS attacks, IDKEYMAN encrypts the identities of publishers using the public keys of subscribers. Tan et al. [11] proposed an Identity-Based cryptographic approach for security in body sensor networks which involves sensors to compute public keys by applying hash function on an arbitrary number of application dependent keys generated by them and stored on their flash memory and perform regular elliptic curve encryption/decryption using Elliptic Curve Digital Signature Algorithm (ECDSA). Their approach not only increases the storage on the flash memory but also incurs higher execution time and energy consumption due to the overhead involved in computing public keys. In contrast, our approach employs similar but simple version of IBE by pre-deploying publishers with the public key of the subscribers and using it to establish session keys for data exchange periodically refreshed at regular intervals.

While the above proposed approaches show significant promise in providing security and privacy support, none have taken into account minimizing the trade-off between energy and security while addressing the key requirements of body sensors such as energy conservation and faster execution, since we believe that energy conservation is crucial for longer life time of the sensors and faster execution is necessary for meeting real-time deadlines. Thus, we attempt to propose such a security solution that strikes a suitable balance between providing robust security and minimizing the execution time and energy consumption of individual body sensors.

Security for publisher-subscriber driven networks was analyzed in [19] and key management based approaches have been proposed in [16], [17] and [18] to ensure confidentiality, integrity and availability. However, the applicability of these networks to a health-care scenario was first investigated by developers of CodeBlue, who utilized this model in their system. We attempt to develop a key management mechanism for CodeBlue system.

III. BACKGROUND

A. *Publisher-Subscriber Architecture*

In this architecture (Figure 1), publishers are the motes attached to the patients and subscribers are their corresponding authorized doctors/care-givers typically holding a PDA/Laptop. Publishers monitor vital body signs of the patients and transmit the data to the subscribers who in turn accordingly initiate responses. On the other hand, a subscriber can also query the publisher real-time for patient's health status. This kind of architecture is mainly suited to a multi cast scenario where data from sender gets sent to multiple receivers to co-ordinate their actions. This scenario is analogous to the health-care environment where there can be more than one authorized doctor/caregiver to diagnose a patient.

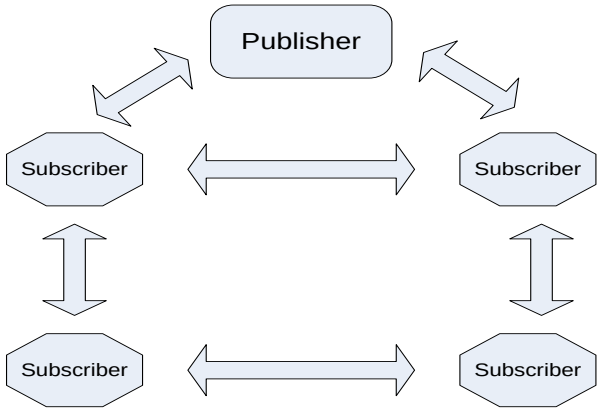

Fig. 1. Publisher-Subscriber Architecture

B. Identity- Based Encryption (IBE)

IBE, a public key based technology (Figure 2) is recently gaining attention among researchers due to rapid key generation and therefore making expensive operations of PKI unnecessary since node's identification information is used as the public key.

Typically nodes obtain their private key using a private key generator on providing its identification information as input. This is feasible compared to trusted certification authority based approach employed in a traditional PKI.

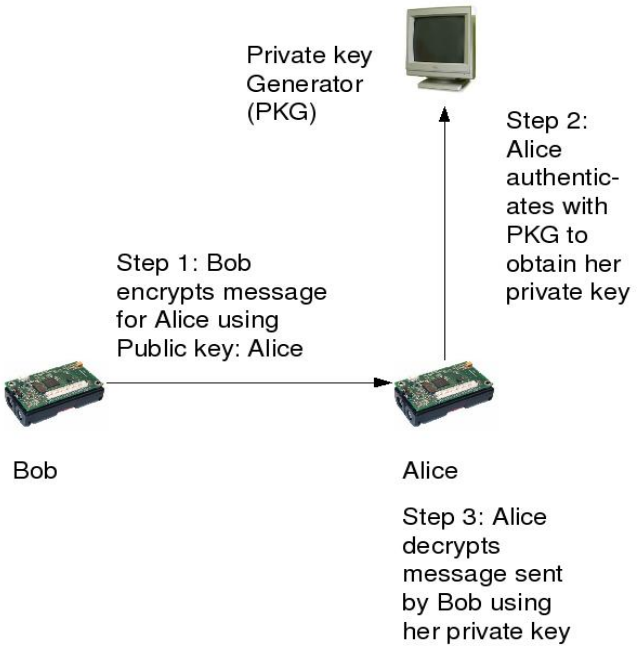

Fig. 2. Identity Based Encryption

IBE is based on Identity based cryptography, initially introduced by Adi Shamir in 1984. We found that traditional IBE incurs greater overhead than symmetric key based approaches [9]. Since, public key based approaches offer the greatest advantage of bootstrapping security, we use IBE only to exchange pair-wise symmetric keys between publishers and subscribers. The symmetric keys are used in subsequent communications thus reducing the computational overhead on the publishers. We elaborate on our approach in the next section.

IV. Proposed Scheme: IDKEYMAN

We assume that authorized subscribers have access to the medical records of their corresponding patients. Our proposed scheme, IDKEYMAN, consists of two parts. We believe that it is necessary to identify and authenticate publishers (patients) during the key management phase. Let us look at the publisher authentication model and the identity based key management scheme below.

A. Publisher Authentication Model

In the publisher authentication model, RFID tags are integrated with wearable medical sensors allowing them to capture a unique identification (PID) of the patients. The publisher gathers the PID information and includes it in the key management scheme (See 4.2) where validation by subscribers takes place before data transfer/communication between publisher and subscriber takes place. Periodic authentication of patients through RFID tags would be essential to increase robustness of the system towards adversaries launching malicious attacks.

RFID technologies have recently been extensively deployed in hospitals [10] and we believe that this mechanism is sufficient to identify patients in hospitals.

B. Identity- Based Key Management Scheme

In accordance with the NIST recommendation on key management [26], our key management scheme (Figure 3) operates in pre-operational, operational, post-operational and destroyed phases.

Pre-operational phase:

We assume that each subscriber is pre-distributed with the private key K_s and public key K_{sub} in addition to a function that takes the ID of the publisher and outputs its corresponding public key. The public key of the subscriber, K_{sub} is programmed in the memory of the publishers. Let us look at the steps outlined below.

Operational Phase:

Step 1: Initially, when the medical sensor attached to the patient is powered on, the mote obtains the patient identification information PID from the RFID tag attached to the patient queried by RFID reader. Once the patient's information PID is obtained, the mote collects PID, its id MoteID, generates a nonce n1, encrypts message using public key of the subscriber K_{sub} and sends it securely to the subscriber. The main objective of using K_{sub} in the first place is to encrypt the patient identification information making it impossible for adversaries to spoof PID. Nonce n1 is included in the message to prevent replay attacks.

Step 2: The subscriber decrypts the received message using its private key K_s and verifies the authenticity of this patient using PID and MoteID. Then it uses received MoteID to derive public key (K_{pub}) for the corresponding publisher, generates pair-wise secret keys, encrypts message using K_{pub} and sends it securely to the publisher. This message contains the ids of both subscriber and publisher, id_s and id_p, pair-wise secret key $K_{p,s}$ along with the nonce that the publisher sent.

Step 3: The crucial part of our scheme is the confirmation from subscriber that publisher has received the correct pair-wise keys before initiation of medical data takes place. After decrypting the message using K_p and obtaining the pair-wise secret keys, publisher sends a message containing its ID and

subscriber's ID encrypted using the pair-wise secret key $K_{p,s}$, which is decrypted by subscriber and confirmed.

Step 4: Now, initiation of medical data takes place by encrypting data using pair-wise secret key $K_{p,s}$ along with the identities of publisher and subscriber and a new value for nonce computed using existing nonce.

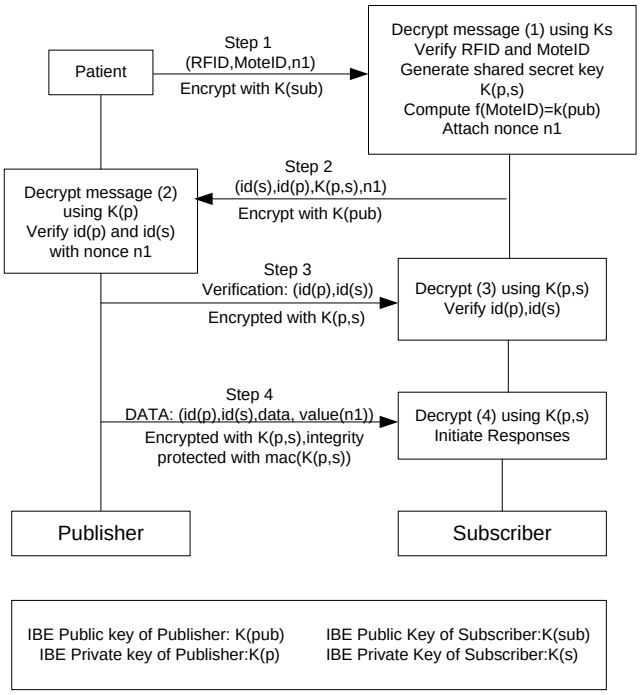

Fig. 3. Identity-based Key Management Scheme

A MAC ($mac_{K(p,s)}$) derived from pair-wise secret key $K_{p,s}$ is used to protect the message from unauthorized message tampering by adversaries. The subscriber decrypts it using the pair-wise secret key $K_{p,s}$ and accordingly initiates responses.

Post-operational Phase:

The pair-wise secret keys are used as session keys for future communications. To update the pair-wise secret keys, the publisher and subscriber exchanges new values of nonces and subscriber computes a new pair-wise key for communicating with the publisher.

Destroyed Phase:

In the destroyed phase, there can be two kinds of cases that need to be addressed with regard to key compromise. If the public key of the subscriber is compromised, we need to re-initialize the expensive pre-operational phase but there exists no other way to fix this issue. On the other hand, if the pair-wise or session key is compromised, initiating the key agreement process will help solve the problem.

V. Security Analysis

We analyze our proposed scheme for resistance against different kinds of attacks relevant to this application. Due to the privacy critical nature of the medical data, identity and data tampering attacks dominate this area of discussion. Impersonation attacks are not possible since only legitimate nodes have access to the public key of the subscriber. Even without impersonation attacks, it is possible that attackers replay old data that may be appropriate for the patients. In that case, we require the subscribers to attach the nonces sent by publishers to prevent replay attacks. Publishers typically buffer their nonces to compare with those received from subscribers to check for consistency. If any kind of inconsistency is observed, the received packet is discarded.

Our scheme preserves the data integrity required for health-care environments apart from confidentiality by computing a MAC on the pair-wise symmetric key to provide increased level of security. Thus any kind of data tampering or false data injection attacks can be detected. Lastly, our scheme requires the generation of different session keys for ensuing communications by exchanging new values of nonces and old keys are erased from memory to prevent key compromise.

VI. Implementation and Performance Evaluation

We have implemented IDKEYMAN in Prowler [12], a MATLAB based wireless sensor network simulator which simulates the Mica2 platform in conjunction with a Pairing Based Cryptography library (PBC) [13] in Perl to implement identity based encryption. We chose AES block cipher for symmetric encryption and SHA-1 for computing the hash function used for MAC. The following are the time and energy evaluations for the proposed scheme.

A. Energy Constraints

We evaluated the energy consumed in IDKEYMAN. Typically, energy consumed by a key management mechanism is determined by the energy required for execution of cryptographic operations along with energy required for transmission/reception. We begin our energy evaluation by computing the energy consumed during execution of cryptographic operations and also during transmission/reception and finally end with stepwise energy computations.

According to [15], we obtained the energy consumption for identity based key negotiation to be 0.44J. The size of each message is set to 512-bits depending on the key length and application headers in our key management scheme. According to [22], the transmission and reception of a single byte of data requires 59.2µJ and 28.6µJ respectively. Thus the transmission and reception of 512-bit message would consume 3.78mJ and 1.83mJ respectively. According to [22], energy consumed by a SHA-1 hash function was 5.9µJ/byte. In our scheme, a 160-bit hash function for computing the identity based public key of the subscriber would consume 0.11mJ of energy.

We used the 128-bit AES cipher for establishing the symmetric key between publishers and subscribers. According to [25], generating a shared secret key using AES cipher consumes 7.87µJ of energy. According to [22], encryption and decryption using AES cipher consumes 1.62µJ and 2.49µJ.

Thus the encryption and decryption of a 128-bit AES cipher would consume 0.025mJ and 0.039mJ of energy. According to [23], computing a MAC using AES consumes 2.31µJ/byte of energy. Thus, computing a MAC using 128-bit AES would consume 0.036mJ of energy.

With the above computed data, we have evaluated the energy consumed at every step of our key management mechanism. Table 1 shows the stepwise energy computations for IDKEYMAN.

TABLE I
ENERGY CONSUMPTION OF IDKEYMAN

IDKEYMAN	Energy Consumed
Step 1	0.44J
Step 2	0.44J
Step 3	5.6mJ
Step 4	5.7mJ
Total Energy	0.89J

B. *Time Constraints*

The following is the time analysis of IDKEYMAN. Similar to energy computation, time taken by a key management mechanism is determined by the time required for execution of cryptographic operations along with time required for transmission/reception.

According to [21], encryption and decryption using IBE takes 35ms and 27ms respectively. We obtained both the transmission and reception times of MICA motes from [29] to be 0.41ms per byte. Thus the transmission and reception of 512-bit message would take 26ms. According to [24], generating a shared secret key for a 32-byte packet using AES takes 2070µs. Thus generating a key using 128-bit AES would take 1.033ms. SHA-1 hash function takes 1.62 ms for computing the hash for 29 bytes of data according to [23]. Thus, a 160-bit hash function for computing the IBE public key of the publisher would take 1.11 ms.

According to [23], encrypting 29 bytes of data using AES takes 2.14ms. Thus, encryption using 128-bit AES would take 1.17 ms. Finally, computing a MAC using AES for 29 bytes of data takes 5.34ms. Thus, computing a MAC using 128-bit AES takes 2.94ms.

With the above computed data, we have evaluated the time it takes to execute at every step of our key management mechanism. Table 2 shows the stepwise time computations for IDKEYMAN.

TABLE II
EXECUTION TIME OF IDKEYMAN

IDKEYMAN	Execution Time
Step 1	0.11s
Step 2	0.12s
Step 3	0.05s
Step 4	0.06s
Total time	0.34s

In our simulations, we considered the subscribers as motes which resulted in similar message generation and verification times with that of the publishers. In reality, since subscribers typically hold PDAs/laptops having computation and communication power significantly higher than that of the motes, we expect this number to go down drastically.

C. *Comparison*

We compare the time and energy consumed in our approach with that of other approaches as shown in Table 3.

TABLE III
COMPARISON OF TIME AND ENERGY CONSUMPTION OF DIFFERENT SCHEMES WITH IDKEYMAN

Scheme	Execution Time	Energy Consumed
Malasri et al. [1]	18.41s	0.11J
Oliveira et al. [9]	0.06s	0.44J
Tan et al. [11]	2.70s	45.66J
IDKEYMAN	0.34s	0.89J

In Table 3, second column is the total time and third column is the total energy needed to generate and verify packets using keys. Table 3 and its corresponding graph (see figure 4) shows that IDKEYMAN facilitates faster key set-up time and at the same time consumes less energy compared with existing approaches. The faster key set-up time and lesser energy consumption is due to using the expensive IBE one-time to set up pair-wise symmetric keys reducing the computational overhead on the motes. Even though [9] executes the fastest consuming less energy, its vulnerability to DoS attacks as mentioned earlier prevents usage in safety-critical BSN. Similarly the higher execution time of [1] and [11] may not be suitable for deployment in real-time systems such as BSN. Further, IDKEYMAN is a complete key management scheme addressing pre-operational, operational, post-operational and destroyed phases. Thus, IDKEYMAN balances robust security with lesser energy consumption and faster execution making it satisfy the prime requirements of BSNs.

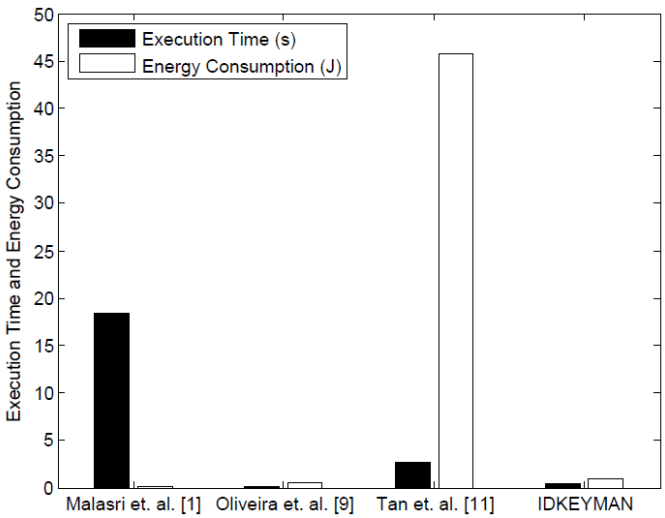

Fig. 4. Time and Energy Comparison with Existing Approaches

VII. CONCLUSION

In this paper, we have provided security and privacy support for publisher-subscriber driven wireless ad hoc body area networks, by presenting IDKEYMAN, a key management scheme using IBE. IDKEYMAN addresses the real-time and stringent resource requirements of individual body sensors while also being robust to attacks. We are currently working to extend this scheme to an emergency response scenario.

REFERENCES

[1] K. Malasri and L. Wang, "Addressing Security in Medical Sensor Networks", In *Proceedings of ACM SIGMOBILE International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments (HealthNet'07)*, San Juan, Puerto Rico, USA, pp 7-12.

[2] V. Shnayder, B. Chen, K. Lorincz, R. F. Thaddeus, J. Fulford and M. Welsh, "Sensor Networks for Medical Care", Technical Report TR-08-05, Division of Engineering and Applied Sciences, Harvard University, 2005.

[3] D. Malan, T. Fulford-Jones, M. Welsh and S. Moulton, "Codeblue: An Ad hoc Sensor Network Infrastructure for Emergency Medical Care". In *Proceedings of MobiSys 2004 Workshop on Applications of Mobile Embedded Systems* (WAMES 2004) June 2004.

[4] L. Eschenauer and V. D. Gligor "A Key Management Scheme for Distributed Sensor Networks", In *Proceedings of ACM Conference on Computer and Communications Security*, pp 41-47, November 2002.

[5] D. Liu and P. Ning, "Establishing Pair-wise Keys in Distributed Sensor Networks", In *ACM Conference on Computer and Communications Security*, October 2003 pp 52-61.

[6] W. Du, J. Deng, Y. S. Han and P. K. Varshney, "A Pair-wise Key Pre-Distribution Scheme for Wireless Sensor Networks", In *ACM Conference on Computer and Communications Security*, October 2003, pp 42-51.

[7] H. Chan, A. Perrig, and D. Song. "Random Key Pre-distribution Schemes for Sensor Networks". In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2003. pp 197-213.

[8] S. Zhu, S. Xu, S. Setia, and S. Jajodia. "Establishing Pair-wise Keys for Secure Communication in Ad hoc Networks: A Probabilistic Approach". In *Proceedings of the IEEE International Conference on Network Protocols (ICNP)*, November 2003, pp 326-335.

[9] L. B. Oliveira, D. Aranha, E. Morais, F. Daguano, J. Lopez and R. Dahab, "TinyTate: Identity-Based Encryption for Sensor Networks", *Cryptology ePrint Archive*, vol. 2007/020, 2007.

[10] H. A. Nahas and J. S. Deogun, "Radio Frequency Identification Applications in Smart Hospitals", In *Proceedings of IEEE International Symposium on Computer-Based Medical Hospitals* 2007. pp 337-342.

[11] C. C. Tan, H. Wang, S. Zhong and Q. Li, "Body Sensor Network Security: An Identity-Based Cryptography Approach", In *Proceedings of ACM Conference on Wireless Security* 2008. pp 148-153.

[12] G. Simon, P. Volgyesi, M. Maroti, and A. Ledeczi. "Simulation-based Optimization of Communication Protocols for Large-scale Wireless Sensor Networks", In *Proceedings of IEEE Aerospace Conference*, Big Sky, MT, March 2003. pp 1339-1346.

[13] P. Miller, "Crypt: PBC Perl module", [Online] Available: http://search.cpan.org/~jettero/Crypt-PBC/

[14] D. Boneh and M. Franklin, "Identity based Encryption from the Weil Pairing". In *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, 2001, pp 213-229.

[15] B. Doyle, S. Bell, A. F. Smeaton, K. McCusker and N. O' Connor, "Security Considerations and Key Negotiation Techniques in Power Constrained Sensor Networks", *The Computer Journal* (Oxford University Press), 49(4): 443-453, 2006.

[16] L. I. W. Pesonen, D. M. Eyers and J. Bacon, "Access Control in Decentralized Publish/Subscribe Systems", *Journal of Networks*, Vol. 2, No.2, April 2007.

[17] J. Bacon, D. Eyers, K. Moodys and L. Pesonen, "Securing Publish/Subscribe for Multi-domain Systems", *Lecture Notes in Computer Science*, Volume 3790, Springer Berlin/Heidelberg, 2005, pp 1-20.

[18] M. Srivatsa and L. Liu. "Secure Event Dissemination in Publish-Subscribe Networks", In *Proceedings of International Conference on Distributed Computing Systems (ICDCS'07)*, Washington, DC, USA, June 2007, pp 22

[19] L. Fiege, A. Zeidler, A. Buchmann, R. Kilian-Kehr and G. Muhl, "Security Aspects in Publish-Subscribe Systems" In *Third International Workshop on Distributed Event-based Systems* (DEBS'04), Edinburgh, Scotland, UK, May 2004.

[20] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, "Perfectly- Secure Key Distribution for Dynamic Conferences". In *Proceedings of Annual International Cryptology Conference on Advances in Cryptology*, 1993, pp 471-486.

[21] Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL). [Online] Available: http://www.shamus.ie/

[22] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks", In *Proceedings of IEEE International Conference on Pervasive Computing and Communications*, 2005, pp 324-328.

[23] J. P. Kaps, "Cryptography for Ultra-Power Devices", Ph.D Dissertation, Department of .Electrical Engineering, Worcester Polytechnic Institute, Worcester, MA, 2006.

[24] H. Cam, S. Ozdemir, P. Nair, D. Muthuaviniashiappan and H. Ozgur Sanli, "Energy Efficient Secure Pattern based Data Aggregation". In *IEEE Computer Communications*, 29:446-455, 2006.

[25] N. R. Potlapally, S. Ravi, A. Raghunathan and N. K. Jha, "Analyzing the Energy Consumption of Security Protocols", In *Proceedings of International Symposium on Low Power Electronics and Design (ISLPED'03)*, 2003, pp 30-35.

[26] E. Barker, W. Barker, W. Burr, W. Polk and M. Smid. Recommendation for Key Management Part 1: General. NIST Special Publication 800-57, March 2007, National Institute of Standards and Technology.

[27] J. Hill and D. Culler, "Mica: A Wireless Platform for Deeply Embedded Networks". *IEEE Micro*, 22(6): 12-24, November/December 2002.

[28] J. K. O'Herrin, N. Fost and K. A. Kudsk, Health Insurance Portability Accountability Act (HIPAA) regulations: Effect on Medical Record Research, *Annals of Surgery* 239, pp 772-776, 2004.

[29] J. Polastre, J. Hill and D. Culler, "Versatile Low Power Media Access for Wireless Sensor Networks", In *Proceedings of ACM Embedded Networked Sensor Systems (SenSys'04)*, Baltimore, Maryland, USA, November 2004. pp 95-107.