VFAST Transactions on Software Engineering
http://vfast.org/index.php/VTSE@ 2014 ISSN: 2309-3978
Volume 5, Number 1, September-October 2014 *pp-01-09*

ECC AND SYMMETRIC BASED HYBRID AUTHENTICATED KEY AGREEMENT IMPLEMENTATION AND ANALYSIS FOR BODY SENSOR NETWORKS

EID REHMAN[1],ASAD[2], ,MUHAMMAD SHER[2]
[1]Department of Computer science & Software Engineering,
International Islamic University Islamabad, Pakistan
eidrehmanktk@gmail.com
[2]Department of Computer science & Software Engineering,
International Islamic University Islamabad, Pakistan
asad@gmail.com, m.sher@iiu.edu.pk

ABSTRACT. *Researcher have made vital and significant out comes in the field of Body Sensor Network (BSN) due to its central role in health monitoring system since last decade. Due to thin-skinned character of its data it desires to maintain confidentiality and magnify security challenges. Key association proposals have unusual interests in BSN because of small tiny nature and daily life usage of these electronic devices. The key role in safe and sound communication is key management practices. Confidentiality, authentication and integrity are achieved by applying key agreement and management methods. Accomplishment of key agreement in BSNs is very daunting task. We proposed a hybrid novel approach with re-keying for BSNs. The symmetric and Elliptic curve cryptography (ECC) based scheme is presented in this paper. The recent researches schemes have privation of security forte, scalability, high communication overhead and computation cost. The security and scalability problems arise, if only symmetric key based scheme apply. Also memory requirement for key storage and high computation cost problem occur, if only public key scheme is applied. Our presented key agreement scheme is depend on symmetric and ECC. We testify our results using NS 2.35 and the result show that the keys storage memory requirement of our proposed scheme reduces from 27% to 47%, computation cost from 50% to 84% percent and communications overhead up to 60% and also provides re-keying features.*

Keywords: Elliptic Curve Cryptography; Key Exchange; Re-keying; Body Sensor Network; Security

1. **INTRODUCTION.** Progressive growth in information technology altered the life style of people. Fast development rationalized the system to look upon each epoch in world. The use and development of technology shifted from battle field to human necessities. Business, Education, engineering and especially Healthiness are main concentrated information technology development domain.

The development of sensor places the world into novel field where all the scientific aspect and solution are scrapped with sensor's realm. Wireless Sensor Network (WSN) made the Communication among these sensor devices. So the developments in WSN lead toward new exciting applications of numerous fields including health caring is one of the important field. The sensors main feature including collecting, processing of data from the environment. WSNs have been used in many favorable applications including habitat monitoring, target tracking and military support operation and emergency response. In WSN medium of communication is wireless, so data is transmitted over wireless medium which needs deployment of security measures. Because of different characteristic and distinct behavior of Human body needs special attention for designing and deployment of sensor network. Therefore, lightweight, miniaturization, cost efficient and tiny sensors nodes are needed in health care field. Because of sensitivity factor of human likes Heart beat

measurement, temperature, and rapid respond and negative impact of non-natural devices to the human tissues, these sensor nodes are design under special consideration. These sensor nodes are attached with human body and communicating with Base station (BS) for updating their information. Base station has large memory, powerful processor, large battery power, communicating all the body sensors and with external network. The sensor nodes transmit data toward medical server where patient data stored which is further connected through external network. Physicians/Doctor read their patient report data by accessing the medical server through internet.
Because of different characteristic of BSN security measures, techniques and its implemented framework are like WSN. The nature of data of medical sensor is sensitive, that way it have different security issues. Protecting and securing the BSN have not been investigated in depth before, so it provides abundant avenue for research study. Because of resource constrain environment the security solution for BSN should take less energy consumption and memory space than universal WSN. In generally, due to the BAN tiny architecture ordinary security solutions should be modified which take less computation and communication cost.

In security technique using cryptography, the key management protocol is the main aspect for ensuring security of communication. For establishing a secure path among nodes and BS and to design cost effective security scheme a key management is the main task. Therefore, in reality key management is the firmest measure of cryptography. The existing key agreement has privation of security forte, scalability issue, high communication overhead and computation cost. A lone usage of symmetric key techniques leads toward scalability and security issues. Key storage and high computation issues occur when public key schemes only apply. In BSN security has been achieved in both schemes, but both schemes need more optimized solution. So a Combination of both schemes leads to overcome the deficiencies of these schemes.
Section 2 consists of different schemes, section 3 includes the proposed scheme, security analysis is presented in section 5 and section 6 consists of simulation and cost analysis.

2. RELATED WORKS.

The author proposed techniques in [1, 3] in which node is preloaded with secrete key and this key is shared among nodes. Sensor node can generate a secret key for communication of certain session using pre shared mechanism of cryptography. These techniques are very convenient where static and non-scalable mechanism is required for huge monitoring and deployment environment of sensor. However, these techniques cannot provision an updating of membership, dynamically change environment and specially cancellation.

For the distribution of symmetric key using public key for mobile ad-hoc network scheme is presented by A. Boukerche and Y, Ren [4]. Because of symmetric key distribution this scheme provides higher security. Public key have been used for protection of shared key which is distribute among sensors. But, due to the high cost this scheme has not been used in BSN.

Biometric scheme based on Bio-channels have been proposed by C.Y. Poon, D. Bao and Y. Zhang [5] for key distribution. Sensor node implanted into the human body and these nodes are linked through Bio-channels. This channel is also used for exchanging keys among nodes. Any biological channel can be hired from these channels for keys management. But the problem is that the biometric system can generate random keys because of dynamic nature of different nodes.

Specific server sharing the encrypted key to all sensors in the network based scheme is presented by W-BAN [6] and AL-NET [7]. This scheme support CC2420 and also based on AES encryption. This scheme accomplishes CCM authentication, CBC MAC and encryption. But the problem in this scheme is that decryption is only made by the BS and also use special platform. The decryption on intermediate node cannot be made using AES decryption.

For generation of cryptography keys, the Inter Pulse Interval has been used in [8]. The peaks of PPG/ECG signal is used for calculation of Time difference and the calculated values then converts into binary for creation of 128-bits key. For the correction of calculated hamming distance Error correction codes are used. This scheme also used random keys and performance of these random keys is faultless. However there are some issues in this scheme. The first one is that error correction codes must be used for keys balancing because of small difference among the Inter Pulse Interval values measured at various sensors. Second on is that higher time requirement for enabling Inter Pulse Interval values for keys leads to very slow mechanism in BSN at real time where the data rate of medical data is too high.

The Master Slave relationship based technique is proposed by Stajano [9]. In this scheme the master device uploading polices to nodes which then allow with other nodes for communication. The main drawbacks of this scheme is dis association among sensor nodes, in which master device disassociate the sensors that comes from prior patient before to reused it for further patient. So, in hospital this scheme is not feasible.
Authentication has been achieved by Jiangal. [10] ,using SCK and ECC to set up pair-wise keys. This scheme used

KDC for loading of top-secret information to nodes and nodes agreed with it based on their identification. For ensuring authentication, node must disclose the secret shared key with at least t nodes. When various ECC curve parameters measures for BSN patient, then association can be achieved. But the issue in this scheme is linking to association mechanism, when there are hundred BSN in a hospital. So the association among sensor and patient could be impractical.

For establishment of pair wise key among BS and sensor nodes ECC has been used by SNAP [11]. In this scheme biometric device is attached with each node for authentication of patient and secrete shared key has been used for communication to BS. The main problem of SNAP is that the establishment of group key can't be requested and the whole authentication process is performed by BS. This leads to more energy consumption and memory of nodes.
Key agreement with re-keying based on Public key cryptography (PKC) has been proposed by M. Conti, R. Di Pietron [12]. This scheme used both DHECC and RSA parameters for keys agreement. This protocol is best for dynamic environment, also providing re-keying feature including key revocation and key addition option. Scalability, resiliency and storage efficiency has been achieved in this scheme using particular routing algorithms in agreement process. However, the main drawback of this method is that it takes large memory and high computation cost because of using both DHECC and RSA.

An optimized computation of RSA for WSN has been proposed in [13]. This Scheme is implemented efficiently and demonstrates that PKC is efficiently applied in WSN. The authors have design a model using cluster mechanism, change the format of packets and also modify RSA. Encryption has been achieved with public key (PK) of cluster head and with PK of BS. BS only performs the decryption of messages. Sensor nodes store the PK of Cluster head and cluster head stores the PK of base station. The experimental result shows that energy consumption is efficient considering various threshold values. Results show that the life time of network is increased. But, due to the encryption of whole domain and PK storage does not apply this scheme to BSN. The communication overhead problem due to the uses of PK for sensors nodes and cluster head, large memory problem and also have high computation cost. There is no well define mechanism for re-keying and also using PK leads to cluster head overloaded problem.

3.**Proposed Scheme.** The topology of Body sensor network is same as shown in figure 1[18]. Because of gateway of scheme [13] have large memory, high energy and powerful processing capabilities we consider it. Routing path table can be constructed by the Gateway according to [16], [17] using deployment information of each node. Cluster scenario formation has been saved using route-selection protocol.

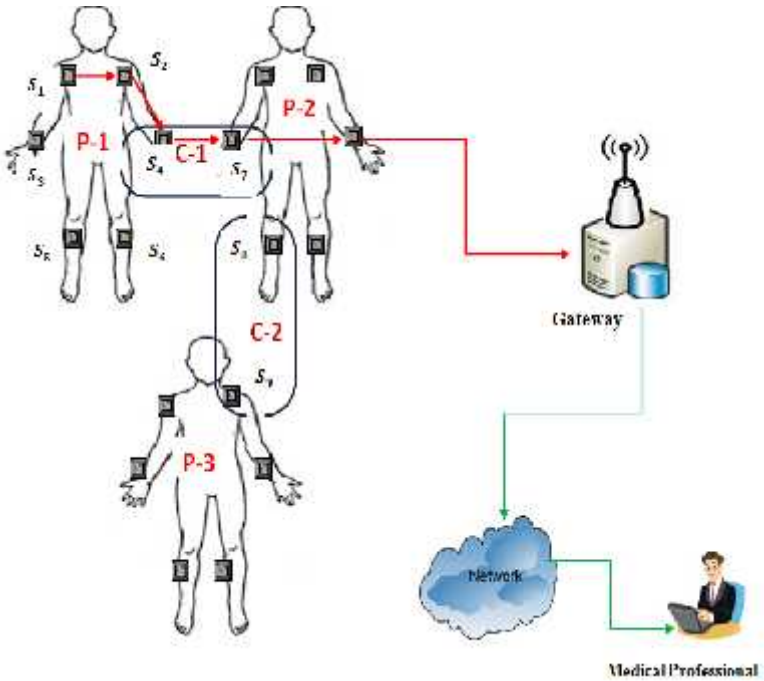

Figure 1: The topology of BSN [18]

Our presented key agreement model is depending on Symmetric and ECC. Our presented model comprises of three phases. First one is the preloading phase before installation of keys, second one is the key establishment session phase and third one is the re-keying phase. The notations used in this paper are given in table 1.

1. q: A large prime number ($q \geq 2^{160}$)
2. C: an Elliptic Curve over prime field Fq of order q
3. G: point of order ($n \geq 2^{160}$) chosen from points on C
4. d_{si}: sensor S_i private key $d_{si} \in \{0,1,2, \ldots \ldots q-1\}$
5. P_{si}: sensor S_i public key $P_{si} = d_{si}G$
6. d_{gw}: Gate way GW private key $d_{gw} \in \{0,1,2, \ldots \ldots q-1\}$
7. P_{gw}: Gate way public key $P_{gw} = d_{gw}G$
8. ID_{si}: Identification of sensor S_i
9. ID_{gw}: Identification of Gate way GW
10. r_{si}: Randomly select number
11. k_{pi}: The shared key for the patients in cluster i
12. k_{Cj}: The shared key for the shared cluster number j
13. E_k/D_k: Encryption / Decryption with key k

TABLE 1: Notation guide

3.1 Keys preloading phase of [18] before installation

The public key of gateway is pre-loaded into each sensor node S_i in the keys preloading phase. Gate way (GW) is pre-loaded with each sensor′s ID_S and its own public and private keys.

Gate way (GW)	d_g , P_g
Sensor S_i	P_w

TABLE 2: Keys preloaded

3.2 Session key establishment phase-I [18]

The below given diagram shows the establishment of session keys in networks using the procedure of figure 2

$S_i \longrightarrow GW \quad E_{P_g}(r_s \parallel ID_s)$

GW:

1. $D_{d_g}(r_s \parallel ID_s)$
2. Compare received ID_s with stored ID_s
3. Randomly select two r_s belonging to the same cluster
4. Compute session key $k_p := (\oplus$ two r_s belong to same cluster i
5. Session key is computed as $k_C = (\oplus$ two r_s belong to same cluster j

$GW \longrightarrow S_i \quad E_{I_s}(k_p \parallel ID_s \parallel ID_g)$

$GW \longrightarrow S_i \quad E_{I_s}(k_C \parallel ID_s \parallel ID_g)$

S_i:

$D_{I_s}(k_p \parallel ID_s \parallel ID_g)$

$D_{I_s}(k_C \parallel ID_s \parallel ID_g)$

Figure 2: Session key establishment diagram of phase-I

1. First a random number r_s is generated by each node S_i and then concatenate it with its own ID_s . After that it is encrypted with public key of gateway using ECC encryption and sends toward gateway GW.
2. When Gateway received the information from sensor S_i, decrypt it and $r_s \parallel ID_s$.
3. Integrity is achieved by Comparing the stored ID_s with the received ID_s for received information.
4. For the generation of cluster Pi session key, two r_s is selected by the gateway from those node S_i whose r_s' belong to the same cluster p_i . same
5. Gateway can generates session key k_p , by taking the XOR of two r_s whose belong to the same cluster i.
6. For the generation of session key k_c for a cluster Ci the gateway calculates the XOR of two r_s belonging to the same cluster j.
7. The sensor node S_i generates session keys k_p and k_c with gateway, k_p and k_c is used by gateway symmetrically encrypted using r_s as a key.
8. Each node S_i use key r_s and symmetric decryption for the decryption of received information.
9. For ensuring the integrity of received information the received ID_s is compare with stored ID_s and ID_g , as integrity is maintain through avalanche effect.

3.3 Re-keying Phase of [18]. Re-keying is performed when a sensor leaves or joins the network or periodic re-keying is performed. In re-keying phase a random number r_s' is generated by each node S_i and the similar procedure will be iterated for keys re-session k_p' and k_c' as in keys establishing phase.

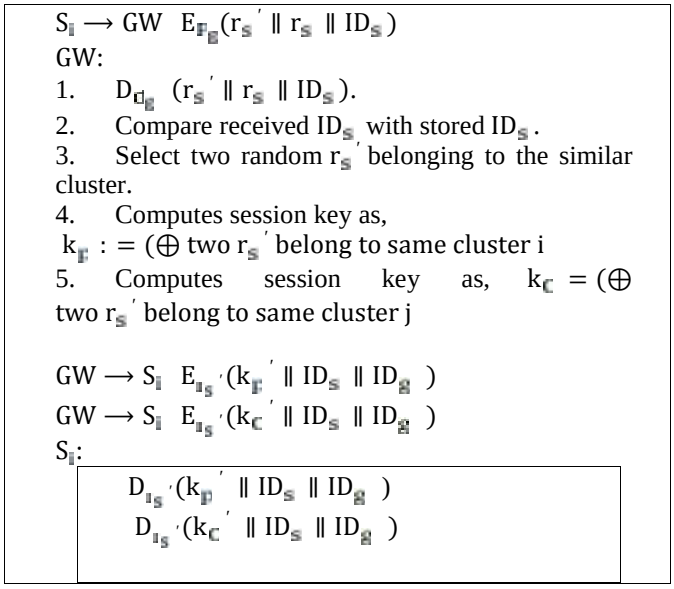

Figure 2: Re-keying phase diagram

3. **SECURITY ANALYSIS.** The analysis below shows BSN security requirements and our technique satisfied these requirements as in [18].

4.1 Confidentiality

During communication, for achievement of data confidentiality information and session key have been exchanged using symmetric cryptography and ECC techniques with enough key size. So our proposed scheme intensely resists cryptanalysis attacks against data confidentiality and key capturing.

4.2 Backward and Forward Secrecy: When a capturing node is detected and a node leave or join a network, the re-keying process is performed in that cluster for ensuring backward and forward secrecy.

4.3 Authentication and Integrity: The gateway compares the sensor stored id with received id after decryption process and sensors compare the gateway stored id with received id. Because of avalanche effect of symmetric cryptosystem and ECC, authentication and integrity is provided through this process.

4.4 Resilience against Captured Node: The public key of gateway is pre-loaded into each sensor node. We presumed that gateway has the detection capability of node capturing as like in [12]. In existence of node capturing, re-keying provide key freshness. So our presented scheme provides good resilience against captured node.

4.5 Scalability. Through re-keying in key distribution process, the proposed scheme has the ability to support the considerable increase in the network size after deployment.

4.6 Implicit Key Authentication (IKA): When gateway ensures that no more sensors except a particular identified node can learn the specific secret key value, then this key establishment protocol is called IKA. Also when key agreement protocol provides IKA to both participant then it is called authenticated key agreement protocol. Our algorithm provides implicitly authentication of information exchanging between gateway and sensors using gateway private key and random no of sensors session key establishment.

4.7 Keys Confirmation (KC): A key agreement protocol is called KC, when one sensor ensured that all nodes have control of a specific secret key through the re-keying procedure and the gateway new established session keys is compared with their similar node self-generation keys. This property fulfills only the steady state (re-keying) phase and this is frequent process. Otherwise for sensors revocation and addition, sensor nodes must trust the gateway and this is referred to the as gateway partial trust.

4. **COST ANALYSIS AND RESULTS.** In our scheme we only emphasis on the performance of sensors and we assumed that the Gateway is resources-rich.
The results based on the simulation (NS2.35) of network model and mathematical analysis. Multiple scenarios and test cases generated on different values according to standards of BSN have been tested. In simulation it is assumed that c number of nodes and their energy is fixed. In mathematical model assumed mathematical calculation for results. As energy is main source of sensor node so our work focused on sensor energy and as we know that GW is rich in resources. The analysis of scheme has been validated according to NIST key standard and other performance measures platform. Proposed model consists upon 20, 15, 10 and 20 sensor nodes in different attempts for comparison of results.

Simulation Parameters	
Parameters	**Standards**
Topology_ area	(500 x 500) meters
Node numbers	05~20
Antenna_ Type	OmniAntenna
Connection Type	TCP
Initial _energy	10J
Data _packet _size	30 Bytes
Tx_ Power	36nJ / bit
Network Components	Interface Queue (IFQ), MAC layer, Link Layer (LL)
Channel Type	Wireless
Physical Type	Wireless Physical
Rx_ Power	36nJ / bit
Routing _Protocol	AODV
Agent Trace	ON
Movemen_Trace	ON

TABLE 3: Simulation Parameter for BSN *IEEE 802.15.6*

Communication cost relative to energy rounds graph for sensor nodes is compared with [13] through simulation as shown below. Our scheme clearly produces efficient result and consumes low energy as in different 5 rounds statistic. Our scheme uses less packet size through smart encryption key size and communication done upon considering different rounds. Our scheme consumes less power of sensor and it's this magnitude goes higher as rounds increases.

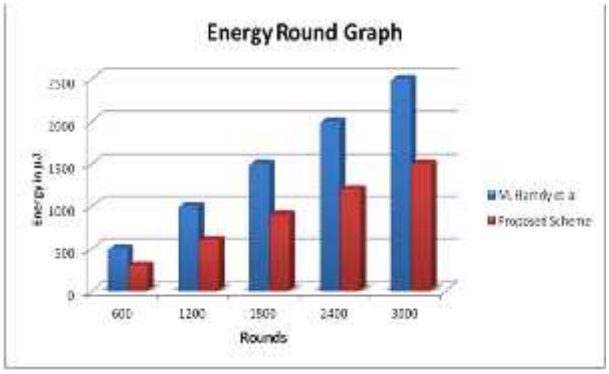

Figure 3: Energy in Rounds

5.1 Key Storage Memory requirement analysis. Because of limited memory of sensor and it is needed that the implementing security scheme should take less memory.

For easiness we use secure key size NIST recommendation and representation of ECC compressed point for ECC, symmetric cryptography and RSA. For same level of security, bits are used as a recommended keys length.

The key length of RSA is greater then 2^1 , Symmetric cryptographic technique key length is greater then 2^1 and ECC key length is greater then 2^1 . The analysis in performed on resources constrained sensor nodes. For easiness our assumption is based on the recommended secure key size of NIST and ECC compressed point representation and for asymmetric and symmetric cryptosystems.

Schemes	**Key stored**	**Approximated key size in bits**	**Memory storage percent reduction**
Scheme [13]	d_s , P_s e, k_E , k_L	160+160+1024+128+128	$\frac{1 \quad -4}{1}$ % = 74%
Proposed Scheme	k_p , k_E , P_E	128+128+160	

TABLE 3: Memory Storage Comparison of Scheme [13] and ECC based Scheme. [18]

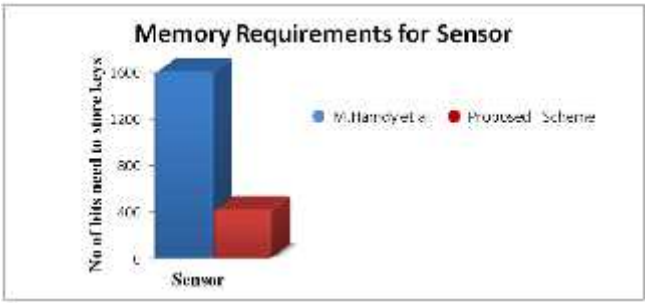

Figure 4: Memory requirement of Sensor

5.2 Analysis of Computation Cost: Elliptic curve point scalar multiplication (ECPM) is one of the expensive and major operations in ECC session key exchange schemes. There are eight total ECPM operation in ECC based Schemes but our proposed scheme has four total ECPM.

RSA and ECC have been proposed in [13] for key exchange. These schemes have four ECPM and two modular exponentiations. As in [15], the private key modular exponentiation of RSA takes approximately while the multiplication of ECC-160 takes only 1.61 seconds. In the presence of these results, the computation cost can be calculates saving as:

According to [18], the saving in computation cost to scheme [13] is

$$\frac{(2 * 22 + 4 * 1.61)s - (4 * 1.61)\,s}{(2 * 22 + 4 * 1.61)s} = 87.23\ \%$$

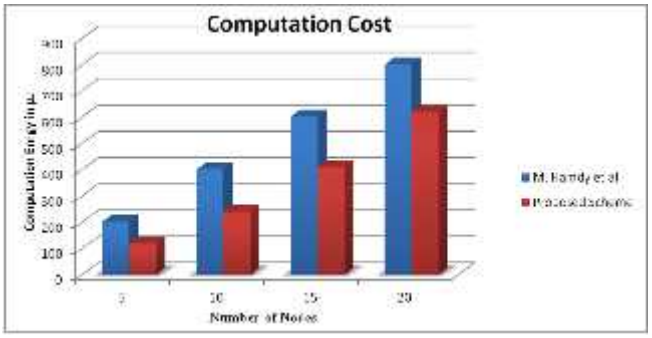

Figure 5: Energy consumption VS No of nodes

5.3 Analysis of Communication Overhead. The uses of bandwidth are the major issue in the BSN. So the less communication cost is efficiency is of greater interest.

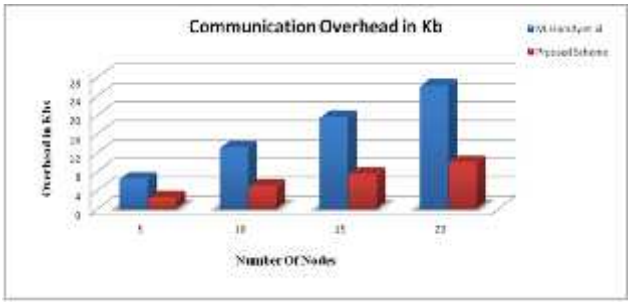

Figure 6: No of nodes and Communication overhead

Schemes	Communication overhead	Percent Reduction in Communication Overhead
ECC based Model Using RSA	(1024+320) bits	[illegible] %= 61.9%
Proposed Scheme	(192+320) bits	

TABLE 4: [18] Communication Overhead Comparison of scheme [13] and proposed Scheme

5. **Conclusions.** Because of limited resources of BSN, the lightweight key management and cryptographic schemes are of greater interest. In this paper Hybrid authenticated key agreement with re-keying for BSN has been proposed in this paper using EEC and symmetric cryptography. The keys storage memory requirement of our proposed scheme

reduces from 27% to 47%, computation cost from 50% to 84% and communications overhead from 20% to 61% and also provides re-keying features.

REFERENCES

[1] Liu, D., Ning, P., & Li, R. (2005). Establishing pairwise keys in distributed sensor networks. ACM Transactions on Information and System Security (TISSEC), 8(1), 41-77.

[2] Liu, D., Ning, P., & Du, W. (2008). Group-based key predistribution for wireless sensor networks. ACM Transactions on Sensor Networks (TOSN), 4(2), 11.

[3] Eschenauer, L., & Gligor, V. D. (2002, November). A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM conference on Computer and communications security (pp. 41-47). ACM.

[4] Boukerche, A., & Ren, Y. (2008, October). The design of a secure key management system for mobile ad hoc networks. In Local Computer Networks, LCN 2008. 33rd IEEE Conference on (pp. 320-327). IEEE.

[5] Poon, C. C., Zhang, Y. T., & Bao, S. D. (2006). A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. Communications Magazine, IEEE, 44(4), 73-81.

[6] Meingast, M., Roosta, T., & Sastry, S. (2006, August). Security and privacy issues with health care information technology. In Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE (pp. 5453-5458). IEEE.

[7] Singelée, D., Latré, B., Braem, B., Peeters, M., De Soete, M., De Cleyn, P., ... & Blondia, C. (2008). A secure cross-layer protocol for multi-hop wireless body area networks. In Ad-hoc, Mobile and Wireless Networks (pp. 94-107). Springer Berlin Heidelberg.

[8] Poon, C. C., Zhang, Y. T., & Bao, S. D. (2006). A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *Communications Magazine, IEEE*, *44*(4), 73-81.

[9] Stajano, F. (2001, January). The resurrecting duckling—what next?. In Security Protocols (pp. 204-214). Springer Berlin Heidelberg.

[10] Jiang, C., Li, B., & Xu, H. (2007, May). An efficient scheme for user authentication in wireless sensor networks. InAdvanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on (Vol. 1, pp. 438-442). IEEE.

[11] Malasri, K., & Wang, L. (2007, June). Addressing security in medical sensor networks. In Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments (pp. 7-12). ACM.

[12] Conti, M., Di Pietro, R., Mancini, L. V., & Mei, A. (2008, March). Emergent properties: detection of the node-capture attack in mobile wireless sensor networks. In Proceedings of the first ACM conference on Wireless network security (pp. 214-219). ACM.

[13] Eldefrawy, M. H., Khan, M. K., & Alghathbar, K. (2010, July). A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography. In Anti-Counterfeiting Security and Identification in Communication (ASID), 2010 International Conference on (pp. 1-6). IEEE.

[14] Sahana, A., & Misra, I. S. (2011, February). Implementation of RSA security protocol for sensor network security: Design and network lifetime analysis. In Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on (pp. 1-5). IEEE.

[15] Gura, N., Patel, A., Wander, A., Eberle, H., & Shantz, S. C. (2004). Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In *Cryptographic Hardware and Embedded Systems-CHES 2004* (pp. 119-132). Springer Berlin Heidelberg.

[16] Lewis, N., Foukia, N., & Govan, D. G. (2008, April). Using trust for key distribution and route selection in wireless sensor networks. In Network Operations and Management Symposium, 2008. NOMS 2008. IEEE (pp. 787-790). IEEE.

[17] Yang, Q., Lim, A., Li, S., Fang, J., & Agrawal, P. (2008, August). ACAR: adaptive connectivity aware routing protocol for vehicular ad hoc networks. In Computer Communications and Networks, 2008. ICCCN'08. Proceedings of 17th International Conference on (pp. 1-6). IEEE.

[18] Asad, M., & Chaudhry, S. A. (2012, April). An authenticated key agreement with rekeying for secured body sensor networks based on hybrid cryptosystem. In Networking, Sensing and Control (ICNSC), 2012 9th IEEE International Conference on (pp. 118-121). IEEE.