A Literature Review: Cryptography Algorithms for Wireless sensor networks

L.Jothi
Department of computer science
K.S.Rangasamy college of Arts and Science College
Tiruchengode-637215, India
jothiloganathan@gmail.com

Abstract*:* **Cryptography is that the observe and study of techniques for secure communication within the presence of third parties. It additionally plays important of wireless sensor networks. The cryptography drawback has addressed in several contexts and by researchers in several disciplines. This expositive paper presents survey of a number of the newest developments on cryptography algorithms in network security and additionally presents with a number of the solutions for wireless sensor network alongside the results.**

Keywords: encryption, symmetric keys, cryptography algorithms, cryptography framework, wireless sensor networks

INTRODUCTION

A literature review is a description of the study relevant to particular field or topic. It is discusses about the information in a particular subject area for the past years. The process of reading, analyzing, evaluating and summarizing materials about specific are called networking, wireless sensor networks(WSNs),cryptography and network security. The review describes summaries, evaluate and clarify various applications of sensor networks in different disciplines. This demonstrates that the knowledge has been gained in the required area and got awareness on the relevant theories.

I.CRYPTOGRAPHY: A REVIEW

Ralph C. Merkle was developed protocols for public key cryptosystems in 1980 [1]. It's used new Cryptographic protocols that take full advantage of the distinctive properties of public key cryptosystems is currently evolving. Many protocols for public key distribution and for digital signatures square measure in short compared with one another and with the standard different.

Mihir Bellare, Ran Canetti,et al was introduced Keying Hash Functions for Message Authentication 1996 [2].The use of cryptographic hash functions like MD5 or SHA for message authentication has become a regular approach in several Internet applications and protocols. Although terribly simple to implement, these mechanisms square measure typically supported ad hoc techniques that lack a sound security analysis. It's present new constructions of message authentication schemes supported a cryptographic hash function. Our schemes, NMAC and HMAC, square measure tested to be secure as long because the underlying hash function has some affordable cryptographic strengths. Moreover it represented, in a very quantitative means, that the schemes retain almost all the security of the underlying hash function. . Moreover they use the hash function (or its compression function) as a black box, so that widely available library code or hardware will be accustomed to implement them in a very easy means, and interchangeability of the underlying hash function is well supported.

In 2004, Philippe Golle , Jessica Staddon and et al presented Secure Conjunctive Keyword SearchOver Encrypted Data [3]. The setting within which a user stores encrypted documents (e.g. e-mails) on an untrusted server. So as to retrieve documents satisfying a particular search criterion, the user offers the server a capability that permits the server to spot precisely those documents. Work in this area has for the most part centered on search criteria consisting of a one keyword. If the user is actually interested in documents containing every of many keywords (conjunctive keyword search) the user should either offer the server capabilities for every of the keywords individually and rely on an intersection calculation (by either the server or the user) to determine the correct set of documents, or alternatively, the user might store extra information on the server to facilitate such searches.

In 2011, vimal upadhyay, pintu kashyap et al.was developed secure data in wireless sensor network via des [4]. It is one in all the most goals of sensor networks is to produce correct information a couple of sensing field for an extended period of time. The emergence of sensor networks jointly of the dominant technology trends within the returning decades has exposed various distinctive challenges to researchers. Because sensor networks could act with sensitive data and or operate in hostile unattended environments, it's imperative that these security considerations be addressed from the beginning of the system design. These networks are probably to be composed of hundreds, and potentially thousands of little sensor nodes, functioning

autonomously, and in several cases. In proposed a number of of the security goal for Wireless Sensor Network. Further, security being very important to the acceptance and use of sensor networks for several applications; we have made in depth threat analysis of Wireless Sensor Network. So, during this paper enforced Encryption Algorithm like - DES to provide sufficient levels of security for shielding the confidentiality of the information within the WSN network. This paper additionally analyzes the performance of DES algorithm against Attacks in WSN Network.

In 2012 Sadaqat Ur Rehman , Muhammad Bilal introduced Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN) [5]. In Wireless Sensor Networks (WSN) have become common day by day, but one amongst the most issue in WSN is its restricted resources. the resources to make Message Authentication Code (MAC) keeping in mind the practicability of technique used for the sensor network at hand. This analysis work investigates totally different cryptographic techniques likes' symmetric key cryptography and asymmetric key cryptography. Furthermore, it compares different encryption techniques such as stream cipher (RC4), block cipher (RC2, RC5, RC6 etc) and hashing techniques (MD2, MD4, MD5, SHA, SHA1 etc). The result of our work provides efficient techniques for communication device, by selecting different comparison matrices i.e. energy consumption, processing time, memory and expenses that satisfies both the security and restricted resources in WSN environment to create MAC.

II.OVER VIEW OF CRYPTOGRAPHY ALGORITHMS FOR WSNs

Dawn Xiaodong Song David Wagner [6], performed Practical Techniques for Searches on Encrypted Data in 2000. It's desirable to store data on data storage servers like mail servers and file servers in encrypted type to scale back security and privacy risks. However, this usually implies that one most sacrifice functionality for security. For this reason, cryptographic schemes are implemented for the problem of searching on encrypted data and provide proofs of security for the ensuing crypto systems. The techniques give obvious secrecy for encryption, within the sense that the untrusted server cannot learn anything about the plaintext it given only the ciphertext. In future work asymmetric key cryptographic techniques will use for providing secrecy and encryption.

Adrian Perrig, Robert Szewczyk et.al introduced [7] SPINS: security protocols for sensor networks in 2002. Basic wireless communication isn't secure. Because it is broad-cast, any individual will pay attention to the traffic, and inject new messages or replay and change old messages. For that reason, this work used a suite of security protocols optimized for sensor networks: SPINS. SPINS has two secure building blocks: SNEP and µTESLA. SNEP (Secure Network Encryption Protocol) provides data confidentiality, two-party data authentication, integrity, and freshness. µTESLA (the "micro" version of the Timed, Efficient, Streaming, and Loss-tolerant Authentication Protocol) provides authentication for data broadcast. In future work, Will victimization AODV or DSR routing security protocols for secure communication.

Hakan Hacıgumus¸ et.al proposed Executing SQL over Encrypted Data in the Database Service Provider Model [8] in 2002. In existing, technique deploys a coarse index that permits partial execution of an SQL query on the provider aspect. The result of the query is sent to the client. The correct result of the query is found by decrypting the data, and executing a compensation query at the client site. The proposed, using Encryption Application service provider is software as a service to a very large client based over the internet. In proposed technique to operate the SQL query, and split it into a server query and a client query. The service provider retains the responsibility to manage the persistence of the data. The client gets total privacy and the cost of cooperating in query execution with the service provider. In future work, will use symmetric encryption technique.

Premkumar Devanbu, et.al [9], developed Authentic Data Publication over the Internet in 2003. Integrity critical databases, such as financial information used in high-value decisions, are frequently published over the Internet. Publishers of such data should satisfy the integrity, authenticity, and non-repudiation requirements of clients. Providing this protection over public data networks is an expensive proposition. This is the difficulty of building and running secure systems. In practice, large systems cannot be verified to be secure and are frequently penetrated. The negative consequences of a system intrusion at the publisher can be severe. The problem is further complicated by data and server replication to satisfy availability and scalability requirement. For this problem merkle hash trees introduced that publishers can use to provide authenticity and non-repudiation of the answer to database queries posed by a client. Merkle hash tree technique is taken a lot of processing time. To resolve this problem, future work will use graph (traveling salesman problem) based techniques

Lingxuan Hu et.al was introduced secure aggregation for wireless networks [10] in 2003. Message aggregation can reduce communication overhead significantly, but message aggregation makes security more difficult. Each intermediate node can modify, forge or discard messages, or simply transmit false aggregation values, so one compromised node is able to significantly alter the final aggregation value. For this problem, new

technique presented a protocol that provides a lightweight security mechanisms introduced to effectively detect node misbehavior (dropping, modifying or forging messages, transmitting false aggregate value). In proposed routing protocols for ad-hoc networks including DSR and AODV. It adopted the μTESLA protocol for authentication of messages transmitted data. μTESLA is a protocol that provides authenticated broadcast for resource constrained environments, it achieves asymmetry from clock synchronization and delayed key disclosure. In future work, will using SUM aggregation algorithm provides the strongest security bound that can be proven for any secure aggregation scheme without making assumptions about the distribution of data values.

Bijit Hore, et.al [11], introduced A Privacy-Preserving Index for Range Queries in 2004. Database outsourcing is an emerging data management paradigm, which has the potential to transform the IT operations of corporations. To address privacy threats in database outsourcing scenarios where trust in the service provider is limited. It analyzes the data partitioning (bucketization) technique and it also algorithmically developed this technique to build privacy-preserving indices on sensitive attributes of a relational table. In the future, work to assess the privacy loss in the case when the adversary has partial information about buckets (which is a more realistic scenario) instead of the worst case scenario.

Wenliang Du., et.al described a key management scheme for wireless sensor networks using deployment knowledge [12] in 2004. In existing, many key agreement schemes used in general networks, such as Diffie-Hellman and public-key based schemes, are not suitable for wireless sensor networks. In proposed technique used Pre-distribution of secret keys for all pairs of nodes is not viable due to the large amount of memory used when the network size is large. In future work, how much the deployment knowledge can improve the q-composite random key pre-distribution scheme and the pairwise key pre-distribution scheme.

Ronald Watro, et.al, was described TinyPK: securing sensor networks with public key technology [13] in 2004. The communication security problems for sensor networks are exacerbated by the limited power and energy of the sensor devices. The critical problem is making effective use of that secure symmetric encryption capability. Public key (PK) technology is a widely used tool to support symmetric key management in the realm of Internet hosts and high-bandwidth interconnections. In this proposed was described the design and implementation of public-key-(PK)-based protocols that allow authentication and key agreement between a sensor network and a third party as well as between two sensor networks. In future work, the problem of supporting mote networks that employ multiple session keys. As mote networks scale to larger sizes, the use of multiple session keys will be inevitable. Mote networks will need to internally generate new keys and deploy them as the communication patterns in the network change.

Michael Gertz April Kwong Charles U. et.al was introduced Databases that tell the Truth: Authentic Data Publication [14] in 2004. The publication of high-value and mission critical data on the Internet plays an important role in the government, industry. However, owners of such data are often not able or willing to serve millions of query requests per day and furthermore satisfy clients' data requirements regarding the integrity, availability, and authenticity of the data they manage in their databases. For that reason proposed work introduced on authentic publication schemes in which a data Owner employs a (possibly untrusted) data publisher to answer queries from clients on behalf of the owner. In addition to query answers, publishers provide clients with verification objects a client uses to verify whether the answer is the same as the owner would have provided. It considered two popular types of database systems, those managing relational data and those managing XML data in the form of XML repositories. In future work Using the GiST(Generalized Search Tree) package are evaluating different types of index structures that can be used for both answering queries and "encoding" Merkle-Hash Tree structures and hash values.

Gunnar Gaubatz, et.al was proposed Public Key Cryptography in Sensor Networks-Revisited [15] in 2004. The common perception of public key cryptography is that it is complex, slow and power hungry, and as such not at all suitable for use in ultra-low power environments like WSNs. For this reason proposed work is symmetric key based message authentication codes (MACs). Two different algorithms: Rabin's Scheme and NtruEncrypt. Rabin's Scheme is based on the factorization problem of large numbers and is therefore similar to the security of RSA with the same sized modulus. Rabin's Scheme has asymmetric computational cost. The encryption operation is extremely fast, however decryption times are comparable to RSA of the same modulus. NtruEncrypt is a relatively new cryptosystem that claims to be highly efficient and particularly suitable for embedded applications such as smart cards or RFID tags, while providing a level of security comparable to that of other established schemes, in particular RSA. In future, work research into energy efficient cryptographic primitives.

Gaubatz,G et.al., was described State of the art in ultra-low power public key cryptography for wireless sensor networks [16] in 2005. In existing, work used symmetric key cryptography. The main problem of symmetric key distribution is that there is no provision for data origin authentication and data integrity protection. For that reason proposed work introduced that special purpose ultra-low power hardware implementations of public key algorithms can be used on sensor nodes. The reduced protocol overhead due to public key cryptography (PKC) translates data into less packet transmissions and hence, power savings. Public

key schemes can be used to provide the security services. It provided an in depth comparison of three popular public key implementations. In proposed work implemented Rabin's Scheme, NtruEncrypt and Elliptic Curve Cryptosystems (ECC) as the most promising candidates for low-power implementations.

Donggang Liu et.al was introduced establishing pairwise keys in distributed sensor networks [17] in 2005. Pairwise key establishment is infeasible to use traditional management techniques such as public key cryptography and key distribution center (KDC). For this reason, the proposed work implemented two efficient instantiations of the general framework: a random subset assignment key predistribution scheme and a grid-based key predistribution scheme. These two schemes provided a high probability (or guarantee) to establish pairwise keys, tolerance of node captures, and low communication overhead. In future work first, the grid-based scheme can be easily extended to a n-dimensional or hypercube based scheme. We would like to further investigate properties of such extensions and compare them with the existing techniques. Second, we observe that sensor nodes have low mobility in many applications. Thus, it may be desirable to develop location based schemes so that the nodes that can directly establish a pairwise key are arranged to be close to each other.

Sencun Zhu et.al Was developed LEAP+: Efficient security mechanisms for large-scale distributed sensor networks [18] in 2006. A key management protocol for sensor networks that are designed to support in-network processing, while at the same time restricting the security impact of a node compromise to the immediate network neighborhood of the compromised node. The design of the protocol is motivated by the observation that different types of messages exchanged between sensor nodes have different security requirements, and that a single keying mechanism is not suitable for meeting these different security requirements. For this reason proposed work introduced LEAP+ (Localized Encryption and Authentication Protocol), a key management protocol for sensor networks. LEAP+ can prevent or increase the difficulty of launching many security attacks on sensor networks. In future work implementing the full functionality of LEAP+ and contributing the source code to the TinyOS community.

Luk, M et.al was introduced MiniSec: A Secure Sensor Network Communication Architecture [19] in 2007. In Existing technologies, such as TinySec and ZigBee, are unable to achieve low energy consumption. For this reason proposed work introduced MiniSec has two operating modes, one tailored for single-source communication, and another tailored for multi-source broadcast communication. MiniSec is a secure network layer that obtains the best of both worlds: low energy consumption and high security.

Giacomo de Meulenaer et.al developed On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks [20] in 2008. Energy is a central concern in the deployment of wireless sensor networks. In this proposed work was investigated the energy cost of cryptographic protocols, both from a communication and a computation point of view, based on practical measurements on the MICAz and TelosB sensors. It is focus on the cost of two key agreement protocols: Kerberos and the Elliptic Curve Diffie-Hellman key exchange with authentication provided by the Elliptic Curve Digital Signature Algorithm (ECDH-ECDSA). It finds that Kerberos is around respectively 20 times and 10 times less costly than ECDH-ECDSA on the MICAz and TelosB. In future work, analysis of the energy gain using ECDH-ECDSA schemes.

Roberto Di et.al was proposed Location privacy and resilience in wireless sensor networks querying [21] in 2010. It provided a probabilistic algorithm and scalable protocol to compute the MAX that enjoys the following features: (i) it guarantees the location privacy of the sensors replying to the query; (ii) it is resilient to an active adversary willing to alter the readings sent by the sensors; and, (iii) it allows to trade-off the accuracy of the result with (a small) overhead increase. As for future work, it is extending the proposed protocol to support other functions, such as range query and top k-query.

Xueying Zhang et.al was developed Energy Efficiency of Symmetric Key Cryptographic Algorithms in Wireless Sensor Networks [22] in 2010. In this proposed, examined the energy efficiency of symmetric key cryptographic algorithms applied in wireless sensor networks (WSNs). It derives the computational energy cost of the ciphers under consideration by comparing the number of CPU cycles required to perform encryption. After evaluating a number of symmetric key ciphers, it compared the energy performance of stream ciphers and block ciphers applied to a noisy channel in a WSN. In future work analyze the ciphers according to their characteristics and the effect of the channel quality when applied in WSNs.

Subhankar Chattopadhyay et.al was introduced A Scheme for Key Revocation in Wireless Sensor Networks [23] in 2010. In existing, Centralized key revocation has a single point of failure. For that reason this work address key revocation scheme based on voting procedure is distributed key revocation algorithm. It represented all the keys of a compromised node can be successfully revoked from the entire network. In future, any other mechanism can be used for voting technique so further reduce the storage cost and time to revoke a compromised node. Also future improvements can be made in terms of reducing the computational and communication cost.

Yang Zhao a, et.al was developed A co-commitment based secure data collection scheme for tiered wireless sensor networks [24] in 2010. Wireless sensor networks are vulnerable to security attacks, especially

the attacks to the storage nodes that buffer and process the data readings from sensors. For this problem proposed introduced a secure data collection protocol (SDC) to support time based queries in tiered WSNs. With small overhead introduced to data communication, SDC protects both data confidentiality and data integrity. A co-commitment scheme to support time based data queries. In the face of data loss, this protocol strives to distinguish with high confidence the security attacks from normal communication signal losses without heavy system overhead. In future work, will use encryption techniques to protect data integrity.

Ashok Kumar Das was introduced a key establishment scheme for mobile wireless sensor networks using post-deployment knowledge [25] in 2011. Establishment of pairwise keys between sensor nodes in a sensor network is a difficult problem due to resource limitations of sensor nodes as well as vulnerability to physical captures of sensor nodes by the enemy. To address the key pre-distribution problem in mobile sensor networks. For this problem proposed scheme introduced a modified version of the key prioritization technique using post deployment knowledge. In this scheme provides reasonable network connectivity and security. In future, further improve the resilience against node capture of the proposed scheme. The improving scheme works for any deployment topology and also supports the addition of new sensor nodes after initial deployment.

Jing Shi was introduced A Spatiotemporal Approach for Secure Range Queries in Tiered Sensor Networks [26] in 2011. In wireless sensor networks, Master nodes collect data from sensor nodes and answer the queries from the network owner. The reliance on master nodes for data storage and query processing raises serious concerns about both data confidentiality and query-result correctness in hostile environments. In particular, a compromised master node may leak hosted sensitive data to the adversary; it may also return juggled or incomplete data in response to a query. For that reason, proposed work introduced a novel spatiotemporal approach (bucketing technique) to ensure secure range queries in event-driven two-tier sensor networks. It offers data confidentiality by preventing master nodes from reading hosted data and also enables efficient range-query processing. More importantly, it allows the network owner to verify with very high probability whether a query result is authentic and complete by examining the spatial and temporal relationships among the returned data. In future work, will use encryption technique for protecting query.

Anderson Santana de was introduced Privacy-Preserving Techniques and System for Streaming Databases [27] in 2012. In this proposed work considered high performance symmetric encryption techniques for greater-than and range queries based on Bloom filters; a system implementation of privacy-preserving event correlation based on MXQuery [maximum query] and a systematic performance evaluation of symmetric encryption techniques allowing equality tests, range queries, and blind addition. In future work how to optimize the key distribution and event generation for different types of queries using proto-filter.

Fei Chen and Alex X. Liu [28], performed Privacy and Integrity Preserving Range Queries in Sensor Networks in 2012. In sensor networks, storage node function act as an intermediate between sensor and a sink for storing data and processing queries. It has been widely adopted because of the benefits of power and storage saving for sensors as well as the efficiency of query processing. The problem of this approach is the attackers hack the storage node. To prevent attackers from gaining information from both sensor collected data and sink issued queries. The encryption procedure is introduced use to encode each data and queries specified by a storage node. This properly by using data encryption standard algorithm. Data encryption standard procedure is not applicable for better security in sensor collected data and sink issued queries. For that reason, future work will use RSA (Rivest Shamir Adleman) algorithm for protecting data and queries.

CONCLUSION

Cryptography plays a vital role in wireless sensor networks and its efficient it very large , compared to that found in review on various cryptography algorithm and its effective various wireless sensor networks. This is not quite enough for wireless sensor networks. So that in future, researchers will go for more number of implementations for the cryptography algorithm methods and their utilities for various wireless sensor networks system.

REFERENCE

[1] R. Merkle “protocol for public key cryptosystem,” in proc, IEEE S&P, 1980 ,pp. 133-134.
[2] M. Bellare, H.Krawczyk, and R.canetti, “HMAC: Keyed –hashing for message authentication,” RFC 2104, 1996.
[3] P. Golle, J. Staddon, and B.Waters, “secure conjunctive keyword search over encrypted data, “ in proc. ACNS,2004,pp. 31-45.
[4] Vimal Upadhyay, Pintu Kashyap, Inder Kumar, Jai Balwan , Lalit Choudhary “ secure data in wireless sensor network via des” International Journal of Enterprise Computing and Business Systems ISSN (Online) : 2230-8849
[5] Sadaqat Ur Rehman, Muhammad Bilal, Basharat Ahmad, Khawaja Muhammad Yahya, Anees Ullah, Obaid Ur Rehman “Comparison Based Analysis of Different Cryptographic andEncryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN)” IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012
[6] Dawn Xiaodong Song David Wagner Adrian Perrig “Practical Techniques for Searches on Encrypted Data” Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on 2002.
[7] Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor WenDavid E. Culler “ SPINS: security protocols for sensor networks” Wireless Networks 8, 521.534, 2002 Kluwer Academic Publishers. Manufactured in the Netherlands.
[8] Hakan Hacıgumus¸ Bala Iyer Chen Li Sharad Mehrotra, “Executing SQL over Encrypted Data in the Database Service Provider Model” in 2002.

[9] Michael Gertz, April Kwong, Charles U. Marte, Glen Nuckolls, "Databases that tell the Truth: Authentic Data Publication", Copyright 2004 IEEE (Volume:16 , Issue: 10)
[10] Lingxuan Hu, David Evans "Secure Aggregation for Wireless Networks " NationalScience Foundation (CCR-0092945 and EIA-0205327) , in 2004
[11] Bijit Hore, Sharad Mehrotra, Gene Tsudik "A Privacy-Preserving Index for Range Queries" Proceedings of the 30th VLDB Conference, Toronto, Canada, 2004 .
[12] Wenliang Du, Jing Deng, Yunghsiang S. Han, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge" in 2004
[13] Ronald Watro, Derrick Kong, Sue-fen Cuti, Charles Gardiner "TinyPK: Securing Sensor Networks with Public Key Technology' Copyright 2004 ACM 1-58113-972-1/04/0010
[14] Michael Gertz , April Kwong , Charles U. Martel, "Databases that tell the Truth: Authentic Data Publication " in 2004.
[15] Gunnar Gaubatz, Jens-Peter Kaps, Berk Sunar, "Public Key Cryptography in Sensor Networks Revisited " Grants No. ANI-0133297 (NSF CAREER Award) and No. ANI-0112889.in 2004
[16] Gaubatz,G., Kaps, J.-P., Ozturk, E. Sunar, B "State of the art in ultra-low power public key cryptography for wireless sensor networks" N SFGrants No. ANI-0133297 (NSF CAREER Award) and No. ANI-0112889. In 2005
[17] Donggang Liu, Peng Ning, Rongfang Li " Establishing pairwise keys in distributed sensor networks" CCS'03, October 27–31, 2005, Washington, DC, USA
[18] Sencun Zhu, Sanjeev Setia, Sushil Jajodia "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks "ACM in 2006.
[19] Luk, M, Mezzour, G. ; Perrig, A. ; Gligor, V. "MiniSec: A Secure Sensor Network Communication Architecture ", Information Processing in Sensor Networks, 2007. IPSN 2007. 6th International Symposium.
[20] de Meulenaer, G, Gosset, F. ; Standaert, O.-X. ; Pereira, o "On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks", Networking and Communications, 2008. WIMOB '08. IEEE International Conference on Wireless and Mobile Computing,
[21] Roberto Di Pietro[a,] Alexandre Viejo[b]"Location privacy and resilience in wireless sensor networks querying" Computer Communications Volume 34, Issue 3, 15 March 2011, Pages 515–523
[22] Xueying Zhang, Heys, H.M. ; Cheng Li ," Energy efficiency of symmetric key cryptographic algorithms in wireless sensor networks", Communications (QBSC), 2010 25th Biennial Symposium.
[23] Subhankar Chattopadhyay et.al, "A Scheme for Key Revocation in Wireless Sensor Networks", International Journal on Advanced Computer Engineering and Communication Technology (IJACECT) in 2010.
[24] Yang Zhao a, et.al ,"A co-commitment based secure data collection scheme for tiered wireless sensor networks" in 2010, Published by Elsevier B.V.doi:10.1016/j.sysarc.2010.05.010.
[25] Ashok Kumar Das," a key establishment scheme for mobile wireless sensor networks using post-deployment knowledge", Published in International Journal of Computer Networks & Communications (IJCNC) Vol.3, No.4, July 2011
[26] Jing Shi, "A Spatiotemporal Approach for Secure Range Queries in Tiered Sensor Networks", Wireless Communications, IEEE Transactions on (Volume:10 , Issue: 1) 2011.
[27] Anderson Santana de Oliveira, Hoon Wei Lim, Su-Yang Yu " Privacy-Preserving Techniques and System for Streaming Databases" in 2012.
[28] Fei Chen and Alex X. Liu , "Privacy and Integrity Preserving Range Queries in Sensor Networks" in Dec. 2012. Networking, IEEE/ACM Transactions on (Volume:20 , Issue: 6)