International Journal of Computer Applications (0975 – 8887)
International Conference on Innovations In Intelligent Instrumentation, Optimization And Signal Processing "ICIIIOSP-2013"

A Secure Key Pre-distribution Scheme in Wireless Sensor Networks using Elliptic Curve Diffie-Hellman Key Exchange

T.D.Ilakkiya
PG Scholar
Department of Computer Science & Engineering,
R.M.K. Engineering College,
Chennai, Tamilnadu, India.

C.Jayakumar, Ph.D
Department of Computer Science &Engineering,
R.M.K. Engineering College,
Chennai, Tamilnadu, India.

T.D.Shobana
Department of Computer Science & Engineering,
PSY Engineering College,
Sivaganga, Tamilnadu,India.

ABSTRACT
Wireless Sensor Networks are often deployed in adverse or hostile environments so there is always a need for key management schemes for sensor nodes. The existing q-composite Random Key Predistribution (RKP) scheme is a probabilistic key management scheme where each node is preloaded with a subset of keys that are randomly selected from a pool of keys. If a pair of neighbor nodes which have at least q common keys can be used to establish a secure link between the nodes. In this paper, we enhanced the previous security analysis (i.e., resilience against node capture) of the q-composite RKP scheme and we present a lightweight implementation of the Elliptic Curve Diffie-Hellman (ECDH) key exchange for wireless sensor nodes Elliptic Curve Diffie-Hellman (ECDH) key exchange which is feasible for resource-restricted sensor nodes. The proposed method ECDH key exchange in WSNs is offering perfect resilience to node capture, excellent scalability, and low memory as well as reducing communication over-head. ECDH is the highly computation-intensive nature of its underlying cryptographic operations, causing fast execution times and with low energy consumption. Our results show that a full ECDH key exchange between two different nodes consumes a normal energy (including radio communication), which is significantly better for high secure environment reported ECDH implementations on comparable platforms.

General Terms
Wireless Sensor Networks, Security

Keywords
Wireless sensor network, security, key management, random key pre-distribution, resilience.

1. INTRODUCTION
Sensors are inexpensive, low-power devices which have limited resources [Akyildiz et al. 2002]. They are small in size, and have wireless communication capability within short distances. A sensor node typically contains a power unit, a sensing unit, a processing unit, a storage unit, and a wireless transmitter / receiver. A wireless sensor network (WSN) is composed of large number of sensor nodes with limited power, computation, storage and communication capabilities. Environments, where sensor nodes are deployed, can be controlled (such as home, office, warehouse, forest, etc.) or uncontrolled (such as hostile or disaster areas, toxic regions, etc.). If the environment is known and under control, deployment may be achieved manually to establish an infrastructure. However, manual deployments become infeasible or even impossible as the number of the nodes increases. If the environment is uncontrolled or the WSN is very large, deployment has to be performed by randomly scattering the sensor nodes to target area. It may be possible to provide denser sensor deployment at certain spots, but exact positions of the sensor nodes cannot be controlled. Thus, network topology cannot be known precisely prior to deployment. Although topology information can be obtained by using mobile sensor nodes and self-deployment protocols as proposed in [Wang et al. 2004] and [Zou and Chakrabarty 2003], this may not be possible for a large scale WSN.

Security in WSN has six challenges: (i) wireless nature of communication, (ii) resource limitation on sensor nodes, (iii) very large and dense WSN, (iv) lack of fixed infrastructure, (v) unknown network topology prior to deployment, (vi) high
risk of physical attacks to unattended sensors. Moreover, in some deployment scenarios sensor nodes need to operate under adversarial condition. Security solutions for such applications depend on existence of strong and efficient key distribution mechanisms. It is infeasible, or even impossible in uncontrolled environments, to visit large number of sensor nodes, and change their configuration. Moreover, use of a single shared key in whole WSN is not a good idea because an adversary can easily obtain the key. Thus, sensor nodes have to adapt their environments, and establish a secure network by: (i) using pre-distributed keys or keying materials, (ii) exchanging information with their immediate neighbors, or (iii) exchanging information with computationally robust nodes.

Since WSNs are often deployed in hostile environments and the data are transmitted over the air, security measures to prevent eavesdropping or tampering of private information are critical. However, due to the resource constraints on sensor nodes, traditional key establishment techniques (e.g., public key cryptography and online key distribution center) cannot be employed. Lightweight and flexible key distribution schemes are essential to secure the communication between sensor nodes.

The network-wide key approach has serious security vulnerabilities; the capture of a single node discloses the common key, compromising all the nodes in the network [1]. To defend against the node capture, in the full pairwise scheme, n nodes in network receives n-1 pairwise keys to communicate with every other node. It assures a high security level against node capture. However, it has a great memory overhead and a bad scalability; the introduction of new nodes in the network is possible only if their keys are preloaded from the beginning [2].

The random key predistribution (RKP) scheme [2] preloads each node with a subset of keys, called a key ring, that are randomly selected from a large pool of keys. Any two neighbor nodes able to find a common key within their respective key rings can use the common key to establish a secure link. Based on the random graph theory, the size of the key pool and the size of the key ring are carefully chosen in order for the secure links to form a connected graph with a high probability. As the existence of a secure link between two neighbor nodes is guaranteed probabilistically, the RKP scheme belongs to probabilistic key sharing. The *q*-composite RKP scheme [3] requires that a pair of nodes have at least *q* common keys to establish a secure link. The *q*-composite RKP scheme is more resilient than the RKP scheme when a small number of nodes are compromised. A key distribution scheme combining the probabilistic key sharing with the threshold secret sharing is given in [4]. Besides

the probabilistic approach, there are a variety of approaches to the key management in WSNs. For more detailed survey on the key management in WSNs, we refer readers to [1], [5], [6].

Resilience in WSNs refers to the resistance of key distribution schemes against node capture. When sensor nodes are deployed in hostile areas (e.g., battle surveillance), an adversary can mount a physical attack on a sensor node and recover secret information from its memory. The resilience can be evaluated by computing the fraction of total network communications that are compromised by a capture of x nodes, excluding the communications in which the compromised nodes are directly involved. Whereas the authors of the RKP scheme [2] do not give a formal analysis of resilience, the formula for the resilience in the *q*-composite RKP scheme [3] is known. In this work, we explore public key cryptography in terms of the Discrete Logarithm Problem, or more specifically, in terms of the Diffie-Hellman Key Exchange Protocol [10], which is the most primitive idea behind public key cryptography. In the Diffie-Hellman key exchange protocol, two users unknown to each other can set up a private but random key for their symmetric key cryptosystem. This way there is no need for Alice and Bob to meet in advance, or use a secure courier, or use some other secret means, to select a key.

2. LITERATURE REVIEW

Wireless Sensor Network (WSN) [Akyilidiz et al., 2002, Estrin et al., 1991] is a kind of network composed of nodes associated with sensors. Each node has the characteristics of small size, limited power, low computation power and wireless access. The sensor node is responsible for collecting and delivering data over wireless network, and it is desirable to keep the delivered data confidential along the wireless transmission path from one node to another. [Tilak et al., 2002, Kong et al., 2001]. To ensure secure peer-to-peer wireless communication [Slijepcevic et al., 2002, He et al., 2003, Heinzelman et al., 1999, Intanagonwiwat et al., 2000, Zhou et al., 1999, Luo et al., 2002, Hubaux et al., 2001, Basagni et al., 2001] the shared session key between any two nodes must be derived [Asokan et al., 2000, Yi et al., 2002, Carman et al., 2000]. Some protocols use a trusted third party to deliver keys to every node [Yi et al., 2003], while other protocols pre-distribute communication keys to all nodes]. [Chan et al., 2003] Since WSNs are self-organized, and trusted third party may not be available, key pre-distribution protocols are often adopted in such networks. However, key pre-distribution protocols need to store session keys in every node. This may be difficult to achieve in a sensor network where thousands of nodes are deployed with limited storage space only enough to store a small number of session keys. It is desirable to design a new key pre-distribution protocol, which can reduce the storage space of session keys for a large WSN without degrading its security. Much research has been done on key distribution in WSN over the past few years. Carman et al. [Carman et al., 2002] analyzed various conventional approaches for key generation and key distribution in WSN on different hardware platforms with respect to computation overhead and energy consumption [Hodjat et al., 2002, Heizelman et al., 2000]. The results showed that conventional key generation and distribution protocols are not suitable for WSN. To cope with the problem, a key management protocol [Carman et al., 2002] is proposed for sensor networks, which is based on group key agreement protocols and identity-based cryptography. This protocol used Diffie-Hellman key exchange scheme to perform group key agreement. However, the high storage and high computation requirements make it difficult to use.Perrig et al. [Perrig et al., 2001] proposed a security protocol for sensor networks named SPINS. SPINS uses base station as a trusted third party to set up session keys between sensor nodes. Liu and Ning [Liu et al., 2003] extended Perrig's scheme and proposed an efficient broadcast authentication method for sensor networks. Their scheme uses multi-level key chains to distribute the key chain commitments for the broadcast authentication. Undercoffer et al. [Undercoffer et al., 2002] proposed a resource-driven security protocol, which consider the trade-off between security levels and computational resources. However, in a randomly dispersed wireless sensor network, the base station is not always available for all nodes. Without the base station, a sensor network using SPINS may be disconnected. Therefore, these schemes are not well suitable for sensor networks due to the need of base station. Eschenauer and Gligor [Eschenauer et at., 2002] proposed a key management scheme based on Random Graph Theory. [Chan et al., 2003, Erdoos et al., 1960, Spencer, 2000].The Random Graph Theory is defined as follows. A random graph $G(n, p)$ is a graph with n nodes, and the probability that a link exists between any two nodes in the graph is *p*. When *p* is equal to 0, the graph *G* has no edges, whereas when p is equal to 1, the graph G is fully connected.

To evaluate the resilience of a key predistribution scheme, one has to compute the probability that a specific key has not been compromised after an adversary captures X nodes. Assume that a sensor node is preloaded with *m* keys (i.e., the size of a key ring is *m*). If $m = 1$ and $X = 1$, then the analysis is straightforward. However, if both *m* and X are larger than one, which is a typical case, various probabilistic events are no more independent and the analysis becomes complicated. We first show that the previous analysis of the *q*-composite RKP scheme [3] does not properly consider the dependency between probabilistic events; a similar inaccurate analysis fora key predistribution scheme can also be found in [4]. Then, we provide resilience in the RKP scheme and the *q*-composite RKP scheme with security in the key management using Elliptic Curve Diffie-Hellman (ECDH) Key Exchange.

3. ORGANISATION

The remainder of this paper is organized as follows. Section 4 explains the random key pre-distribution schemes [2], [3]. Section 5 presents new enhanced security analyses of the *q*-composite RKP scheme with ECDH. Section 7 concludes this paper.

4. RANDOM KEY PRE-DISTRIBUTION SCHEMES

A random key pre-distribution scheme consists of three phases: (1) initialization, (2) shared-key discovery, and (3) path-key establishment. In the initialization phase, a large pool of keys *S* is generated. For each sensor node, *m* keys are randomly selected from the key pool *S* and stored into the node's memory. After the sensor nodes are deployed, a shared-key discovery is performed where each node tries to discover its neighbor nodes with which it shares common keys. Let $k_1, k_2 \ldots k_i$ be the common keys shared by two neighbor nodes. In the RKP scheme, a link key *K* is chosen randomly from the common keys $k_1, k_2 \ldots k_i$. In the *q*-composite RKP scheme, if $i \geq q$, a link key *K* is generated as the hash of all common keys, i.e., $K = \text{hash}(k_1 \| k_2 \| \ldots \| ki)$. Note that the 1-composite RKP scheme (i.e., $q = 1$) is different from the RKP scheme; while the link key in the 1-composite RKP scheme is the hash of all common keys, the link key in the RKP scheme is equal to a single key that is chosen from the common keys. After the shared-key discovery is completed, two neighbor nodes may not have a link key because their key rings do not have enough common keys. When the two nodes need to establish a secure communication, they can setup a path-key by finding a multihop

secure path between them. If the graph of secure inks is connected, a path always exists between any two nodes.

Let *p* be the probability that a link key can be set up between two sensor nodes during the shared-key discovery and let *d* be the expected degree of a node, i.e., the expected number of secure links a node can establish during the shared-key discovery. From the random graph theory [2], [7], it is known that in order for the secure links to form a connected graph with a high probability *c*, the expected degree *d* should satisfy the relation

$$d = p * (n-1) = \frac{(n-1)ln(n) - ln(-ln(P_c))}{n} \quad \ldots\ldots..(1)$$

where *n* is the total number of nodes. Let *n* be the expected number of neighbor nodes within communication radius of a sensor node. Since

the expected node degree must be at least d as calculated, the required probability p of successfully performing the shared-key discovery with a neighbor node should be

$$p = \frac{ln(n) - ln(-ln(P_c))}{n} \quad \text{.....(2)}$$

5. Q-COMPOSITE DATA DISTRIBUTION WITH ECDH

The Q-Composite Data distribution to create the number of nodes and each and every node can find the security in every sending (Time) and receiving (node probability) process. The key management scheme which is used to exchange the key between ECDH nodes. It is assumed in the WSN that each node will accurately forward messages to Key management to identify whether all the sensor nodes exchange the key securely or not.

Key management is the managing process of security keys in ECDH. It also deals with key exchange, storage and replacement of the keys. Key management concerns with the user level, either between nodes or systems. The Key will be exchanged between nodes randomly and securely. Exchange to any secured communication, nodes must setup the details of the ECDH System.

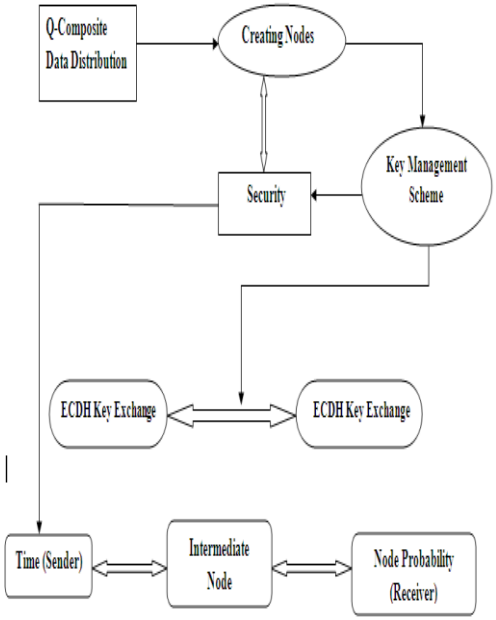


Fig.1 q-Composite Distribution

The implementation of random key pre-distribution with ECDH for checking the valid keys, Nodes, Path and Security for every sending and receiving process is shown as context diagram in Fig.2. The process can still run in the key management schemes for validation. The ECDH key management Scheme checks all the validation method and again to continue key exchange for nodes.

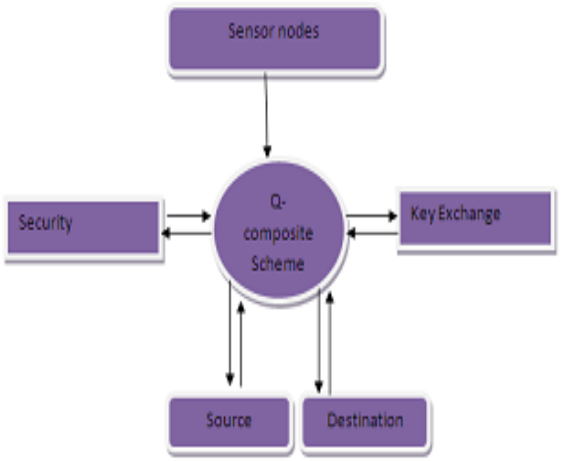
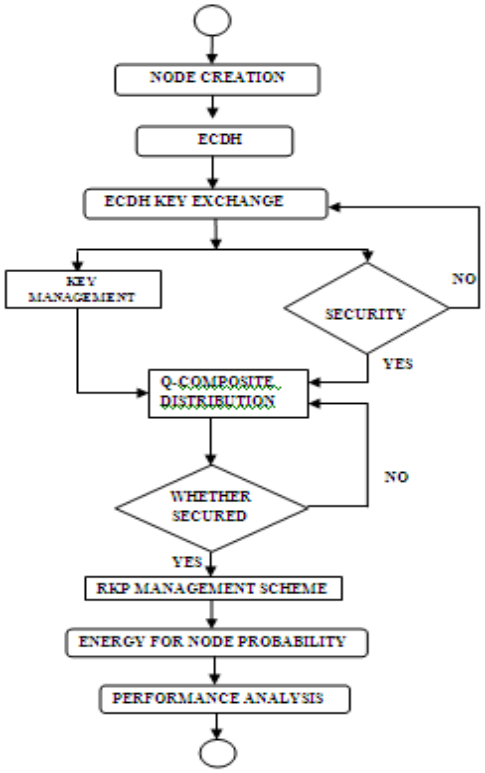


Fig.2 Context Diagram



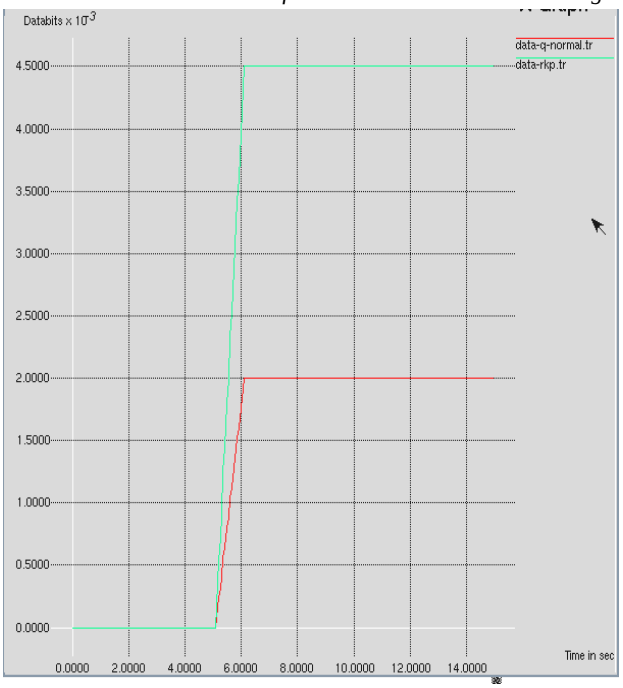


Fig.3 Data Flow Diagram

Fig.4 Performance level based on Data Rate

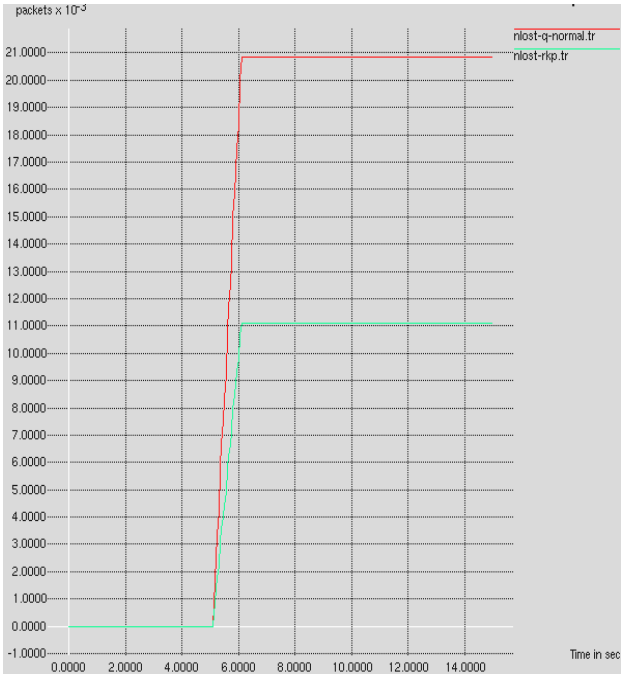


Fig.5 Performance level based on Packet Transfer

6. PERFORMANCE ANALYSIS AND DISCUSSIONS

This section deals with the performance analysis of q- composite, q-composite with RKP scheme with ECDH and the performance analysis are shown as graphs generated in Network Simulator 2.0. There are four parameters considered as the performance metrics. They are data rate, number of packets transferred, Delay incurred in sending packets and the energy usage while providing enhanced security with ECDH.

Fig.4 shows the Performance level based on Data Rate. In X axis time is taken in seconds. In Y axis the data rate is taken in bits. The performance of the data rate can be increased in the Random Key Pre distribution scheme (RKP) with ECDH. By increasing the data flow rate from one node to another node the bandwidth of a wireless channel can be effectively used for further transmission of packets.

Fig.5 shows the performance level based on the transfer of packets. In X axis time is taken is taken in seconds. In Y axis the packets can be taken. The performance level of the packet transfer can be increased by using the RKP scheme with ECDH. Here the number of packets transferred by our proposed scheme is doubled when compared with q-composite scheme.

Fig.6 shows the Performance level based on delay incurred in the transmission process. In X axis time is taken in seconds. In Y axis the data rate is taken in bits. The proposed schemed decreases the delay when compared to q-composite scheme.This increases the throughput of the network.

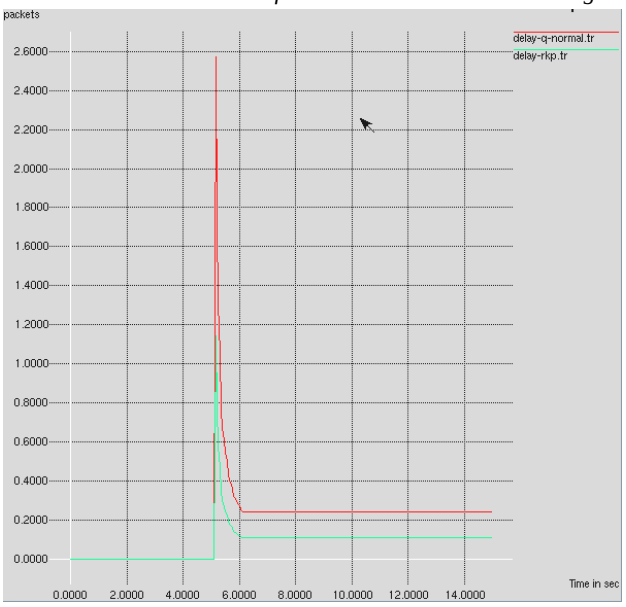


Fig.6 Performance level based on Delay

Fig.7 shows the performance level based on the usage of energy. In X axis time is taken in seconds. In Y axis energy is taken in joules. Because of applying security algorithm, the amount of energy usage is increased but it is in the affordable range.

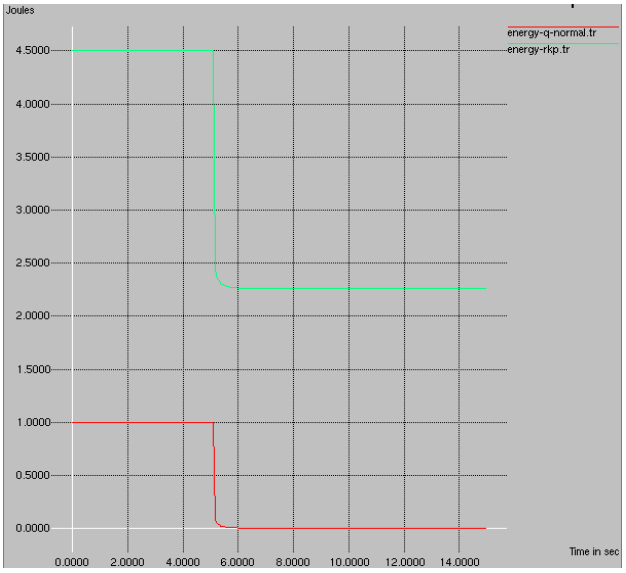


Fig.7 Performance level based on energy usage with ECDH

7. CONCLUSION AND FUURE ENHANCEMENT

We show that the analysis of the *q*-composite RKP scheme with ECDH is secure even though the energy consumption is higher but within affordable range for wireless nodes compared to previous schemes discussed in literature. In future this work can be extended with various security algorithms to further improve the security as well as reduce energy consumption.

8. REFERENCES

[1] M. A. Simplıcio, P. S. L. M. Barreto, C. B. Margi, and T.M. B. Carvalho, "A survey on key management mechanisms for distributed wireless sensor networks," Computer Networks vol.54, no. 15, pp. 2591– 2612, 2010.

[2] L. Eschenauer and V. D. Gligor, "A key-management scheme for dis-tributed sensor networks," in Proc. 2002 ACMConference on Computer and Communications Security, pp.41–47.

[3] H.Chan, A. Perrig, and D.X. Song, "Random key pre-distribution schemes for sensor networks," in Proc. 2003 IEEE Symposium on Security and Privacy, pp. 197–213.

[4] S.Zhu, S. Xu, S. Setia, and S. Jajodia, "Establishing pairwise keys for secure communication in adhoc networks: a probabilistic approach," in Proc. 2003 IEEE International Conference on Network Protocols, pp. 326–335.

[5] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway,"A survey of key management schemes in wireless sensor networks,"ComputerCommunications.,vol.30,no.11-12,pp.2314–2341, 2007.

[6] P. Bose, H. Guo, E. Kranakis, A. Maheshwari, P. Morin, J.Morrison, M. H. M. Smid, and Y. Tang, "On the false-positive rate of Bloom filters," Inf. Processing Letters., vol. 108, no. 4, pp.210–213, 2008.

[7] K. J. Christensen, A. Roginsky, and M. Jimeno, "A new analysis of the false positive rate of a Bloom filter," Inf.Processing Letters vol. 110, no. 21, pp. 944–949, 2010.

[8 "Diffie- Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups," Ayan Mahalanobis, Florida, August 2005.

[9] ECC over RSA for Asymmetric Encryption: A Review, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011