IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 2, Ser. 1 (Mar. – Apr. 2025), PP 11-17
www.iosrjournals.org

Optimized Key Management Scheme Based On Hashing And PSO Algorithm For WSN

Dr. B. Hari Krishana
Assistant Professor,
Manpower Development College, Moula-Ali, Secunderabad, Telangana, India

Abstract:
Wireless sensor network are collection of many autonomous nodes or sensors that communicate to each other without any infrastructure. The sensors have the capability to collect information or message and pre-processing and send it to a base station for further processing. A WSN network operational in a battle zone, we must encode every data or information from source node to destination node and it's vice versa. So, security of data transmission is the main constrained issue in WSN, in this paper we discuss all the issues and challenges in WSN in security aspect. We provide a framework for data security and key management In order to attain data secrecy in such an atmosphere we develop a cluster key which should be updated whenever a node is conceded. A tree based key management scheme need to be used which should compute the new set of key and distribute to cluster members effectively in the context of storing, transmission and processing.

Date of Submission: 22-02-2025 Date of Acceptance: 02-03-2025

I. Introduction

Spatially distributed autonomous sensors are being used in the Wireless Sensor Network so as to control and predict the conditions like temperature, pressure, sound, etc. and at the same time data is being transferred to the respective locations via the particular network. In t5he modern network the bi-direction property is being optimized which also go for the various sensor activities. There are various applications which gave birth to the wireless sensor network like military activities which also includes the surveillance of the battlefield, and also the wireless application is serving in many more industries too like health which includes the monitoring and the control as well.

WSN is defined as the group of the nodes which may vary from hundred to thousands too, each available node in the network is connected to at least to a sensor or sometime to many sensors too. Nodes available in the network is composite attribute which includes many parts like radio transceiver, microcontroller, electronic circuit along with power source, each part of the node performs different function like catching and broadcasting providing power to the node, etc. Size of the sensor node cannot be defined it can vary from the size of dust grain to the size of the shoebox, and the further research is on-going for the microscopic nodes which cannot be seen by naked eyes. Likewise the size of the sensor node the cost of the node may vary from to hundred of dollars, the cost of nodes is decided on the basis of the complexity of the work done by the sensor node. Many network related factors of the network are depended on the cost and size of the sensor node like bandwidth, power requirement, memory and speed. The physical connection of the sensor nodes which is also termed as the topology may be as simple as star connections and may go to the complex level of multi hop mesh network. Hopping and routing are the two possible propagations techniques between two hops.

II. Application

Besides the complexity of the WSN it has wide range of applications in various fields where information sharing is important like military, medical fields, disaster areas, etc. Wireless ad-hoc network is being required in the robot acquisition system for the purpose of sharing the information. Entertainment field also uses the WSN for sharing the music, games, video and other related data. Various study are being shared from one to another by the means of the WSN. Important information is being shared in the surveillance system using the WSN. Hence above are the application of the WSN for various based on the field in which the WSN is used.
In fig. 1 we can see the several applications where we used wireless ad-hoc network very frequently.

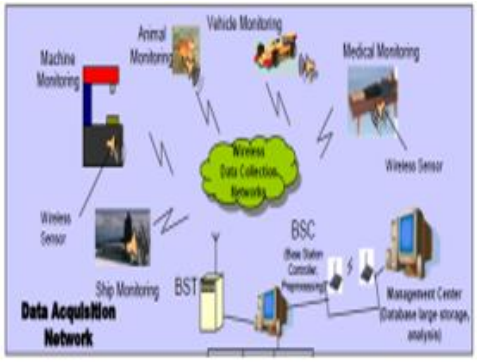

Fig.1 Application of Wireless Sensor network.

As the number of fields in which the wireless network can be used is increasing which increases the popularity of the Wireless Sensor Network in various fields of its application area. Ad-hoc network is used in the applications area where networking infrastructure is not available or is quite costly to install the same and provides the networking conveniently. As the ad-hoc netwok is the group of spreaded nodes and hence it is quite easier to make changes to the network either by removing or inserting new nodes in the network. The set of applications for MANET is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources.

- Military battlefield: Computer peripherals and other computer related equipment's are the part of military services know and hence the wireless sensor network is best suited so as to connect the peripherals among each other and military can take the advantage of common place networking scheme using the wireless networking. The wireless scheme can be used to pass the information or better connect the vehicles, soldier, and base station of the military. As per the study the military was the first to use the type of wireless network on the field.
- Commercial Sector: In the disaster management and in the rescue operations fast and easily deployable network is required and the Ad-hoc network fulfils the requirements and can be used in the conditions like flood, earthquakes, fire, etc.
- Local level: Ad hoc networks can be used in local level like classrooms, seminar halls, conference hall etc. Another local level application of ad-hoc network could be home network where device can communicate directly to share information. With the help of MANET the device can easily connect with other devices like printer, projector, laptop etc. easily and quickly.
- Collaborative work: In some business environment the collaborative work is very necessary even outside of the office therefore a communication medium is required with fulfil the requirement. Any office employee can share useful information with other using MANET.

III. Related Work

Because of the widespread use of the wireless network in various field where information sharing is the critical task hence the factor security became the hot topic for research. X. Cao et al. presents the security solution [4] termed as resource oriented security solution (ROSS) which secures the network from the sensor network which are heterogeneously clustered. As per the study and results of the ROSS it is proven that the algorithm not gives the well-defined security but also provides the trade-off among the security and cost of the performance.

In H.W. Chan et al. work [5] the problem of bootstrapping was solved by three new mechanisms which provides the framework for key distribution which are randomly distributed, namely the q-composite structure, the multipath reinforcement approach, and the random pairwise scheme. Different scheme for the key distribution is being presented in all three mechanism presented or we can say protocol is being presented for the key distribution. Eschenauer et al. developed a new key distribution mechanism for the distributed wireless network [6]. The mechanism presents the theme which fulfils the requirement of the security and operation of the network as well. Basically the mechanism is for sharing the key among nodes using probability on random graph and simple protocols are being followed for key establishment and path making, and other activities are handled like re-keying, key revocation and adding nodes to the network.

Q. Gu et al. presented a mechanism [7] for broadcast large sensor networks and so as to take complete advantage of the available nodes in the wireless network, and also provides an alternative way to the tradeoff between the delay in verification of the nodes and broadcast overhead so that the different requirements of the various applications can be satisfied. In [8] presented a new mechanism so as to provide a beneficial protocol for session key sharing in sensor network. As the negotiation of the key is not depended on the number of nodes in the sensor network hence it has greater scalability while simulating the mechanism. As the number of transmission

are being reduced which affects the power consumption. C. Zhang et al. Provides the description of the various security features of the ad-hoc network [9].

IV. Problem Statement

Security of data in SGC framework can be attained by shared key used by the set of sensor nodes. When shared group key is shared for secure transmission, if any sensor is negotiated, we require to modify the shared key, in order to attain onward access control that means the malicious node should not be capable to decode further data). The procedure of changing the shared key and issuing it to cluster members is known as rekeying. Rekeying is essential in SGC to confirm that only present sensor nodes in the topology can transmit confidentially. Dimension of the rekeying data is nothing but numeral of encodes are essential to allocate the different common key to the sensor nodes in the topology confidentially. The basic or effective approach used to share the secure key between the nodes is by assigning it initially to each sensor node before network establishment. However this mechanism will not permit group changing aspects. The various kind of key distribution and organisation methods which have been discussed in common network surroundings are as noticed in [16]. The various methods permit each sensor network to commonly create and modify local shared group keys and combined with other group to create a unique network group key as discussed by different author [16, 17, 18]. When the dimensions of the sensor network increase then the transmission and processing overhead increases in distributed phenomena.

The concept of key management for shared communications in general network systems are discussed in [18, 19, 20, 21, 22]. A.K. Wong et al. proposed an effective tree based key management approach known as LKH (Logical tree Hierarchy) [23]. In this methodology modification of key required O(log2N) messages where N is the size of the group. According to author each node has to keep log2 N keys and the key server has to maintain a tree of O(N) keys. The methodology [24] projected by A. Kadlur et al. uses the Logical tree Hierarchy approach and uses a binary tree, but this approach requires only two keys at each level instead of log2N keys. This decreases numeral keys at the server from O(N) to O(h) where h is the height of the tree. However storing at each node rests at O(log2 N). The approach deliberated in [25] update the structure proposed by Kadlur [24] to m-ary tree rather than binary tree, which decreases the storage requirement at user end from O(log2 N) to O(logm N) as discussed in [24]. In tree based key management policy private key with the key server share with each node and key at the root of the tree and shre by the each node of the group known as group key. Additional keys (different from private key and group key) are known as auxiliary keys (key encryption keys) which are recognised only for specific subgroup of users and are used to encode modified group key when there is a group membership change.

V. Proposed Work

WSN is the group of n number of sensor nodes arranged as m-ary tree where the leaves of the tree are representing the sensor nodes of the network as represented in the figure 1. The complete network represented as m-ary tree is handled by a central node. In tree represented each part has its role play as the GK (group key) at the origin of the tree are used to encode the information in the circulation. Sensor nodes represented at the leaves of the tree shares the private key to the central node so as to communicate to the central node termed as the private key of the communicating node and rest of the keys are shared through the available path and are termed as auxiliary keys and are used so as to encrypt the key new generated keys. At the time of updation of the tree means any new node enters the communicating area the tree updates the group key and shares it with the rest of the available nodes with secure transmission mode. [25] defines the methodology to have the encryption keys so as to encrypt the newly generated keys for sharing with other nodes. After the generation of the encryption keys the group keys generated are shared with the available nodes in the network without testing the working reality of the keys. When new group reaches the sensor nodes the auxiliary keys also changes or is computed. The available keys are stored in the route from the leaf to the root by every available sensor nodes.

Every node:

1. Has the ability to calculate a one-way hash function H as discussed in [26, 27].
2. is able to update auxiliary keys after getting new group key using the function F as follows:

F(auxiliarykey, newgroupkey) □(Auxiliarykey) XOR (NewGroupkey).

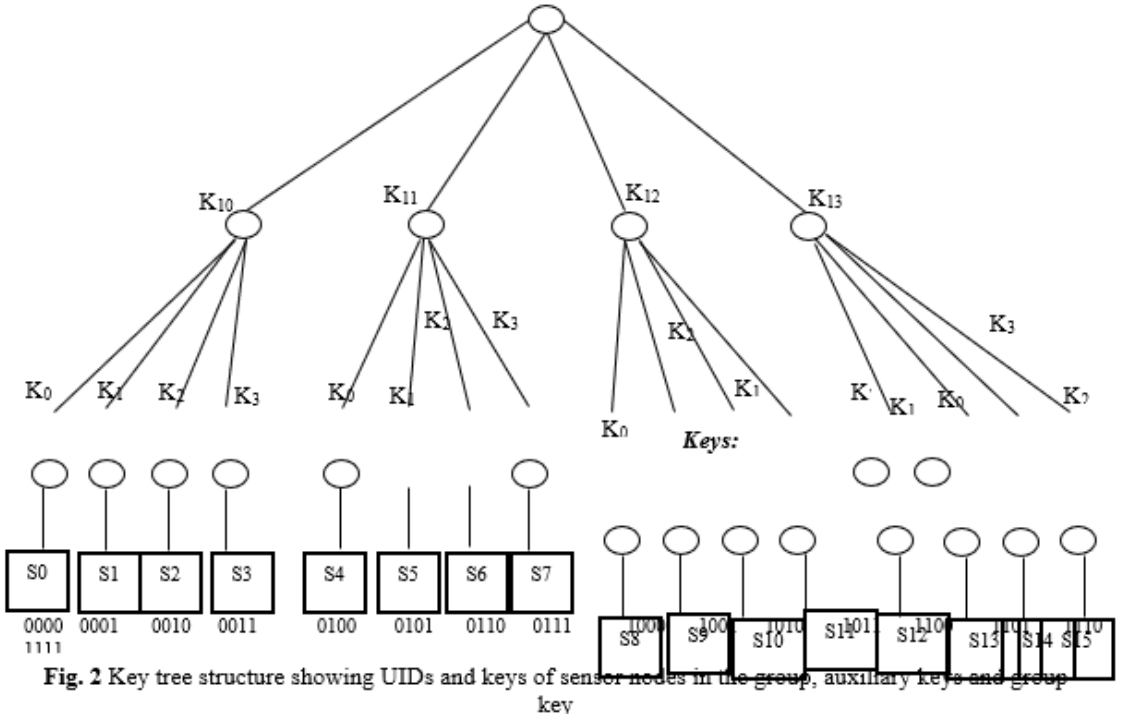

Fig. 2 Key tree structure showing UIDs and keys of sensor nodes in the group, auxiliary keys and group key

Above Fig. 2 show the Key tree structure presenting UIDs and sensor keys in the cluster, auxiliary keys and group key

The keys commonly used by sensor nodes s0 to s15 are the group keys GK.

m-ary tree: has the below mentioned characteristics:

- Interior nodes can only have m Child
- The length of the available paths from the leaf to the root should have the same length
- N: the sensor nodes are associated at the leaf part of the tree. A UID (unique identification number is being given to each node represented in the form of the binary string of length m (where x=log2N).

Subgroups: The interior allowed to have maximum m child and any interior with m nodes is termed as a subgroup.

Keys: In any subgroup the keys are numbered from K0 to Km-1 and as the result of that the sensor nodes at level 0 are assigned with keys K0 and so on to Km-1 in any subgroup.

Figure 1 defines the values of the different available keys or the values of N, m, x, and other keys as N=16, m=4, x=4.

Sensor nodes s0, s4, s8, s12 are assigned with key K0
Sensor nodes s1, s5, s9, s13 are assigned with key K1
Sensor nodes s2, s6, s10, s14 are assigned with key K2
Sensor nodes s3, s7, s11, s15 are assigned with key K3
K10, K11, K12, K13 are auxiliary keys at level 1.

Encryption to Hashing

The method of encryption is being replaced by hash function and the working after replacing is as follows: the central node responsible for controlling the rest of the tree will generate the hash [26] [27], for the shared keys which is only identified by the central nodes and the nodes which are authorised for that, say ks i.e., H(ks) of the encryption key and XOR's with novel undisclosed key knew to be transferred (kcomm ← H(ks) ⊕ knew). Upon receiving k comm nodes having ks compute H(ks) and XOR's with kcomm which yields new secret key knew (knew ←H(ks) ⊕ kcomm). As per the method represented if any two nodes gets the same keys which are taken as secret then the two available node is eligible for generating the hash for other node, this all is under single communication. For e.g., a node say gx having ks can recuperate H(k0s) as follows : H(k0s)← (H(k0s)⊕ knew)⊕ knew where knew is recognised to the node and H(k0s)⊕ knew is eavesdropped. Using the above method the secret key can be decrypted by hash H(K0s) for the node gx in the upcoming communication.

Each hash is being increased by one so to avoid the above condition and then it is allowed to proceeds next hash value for the further transmission means K0=K0+1. It is operationally unlikely for a user for the duration of the ith application of this approach to recover k0s+i even given H (k0s+i), . . .H (k0s). The overall method is secure due to the property of one way hashing of the function as per [26][27].

Hash-Based Key Distribution Method

Without testing the ground working of the newly generated encrypted keys are shared and are then used so as to communicate to the other groups, keys are being encrypted using the method in [26]. Taking the tree in fig. 1 into consideration. If s5 and s6 are the compromised sensor nodes then as per the above method the keys are KEK={K10, K12, K13, K0, K3}. As per the hash method in the previous part the rest of the keys are being distributed to the rest of available nodes. To communicate new group key GK0 to nodes s0, . . . , s3 central node computes the hash of key k10 i.e., H(k10) and XOR's this with new group key GK0 which yields Ks0,...,s3 ← H(k10) ⊕ GK0. Upon receiving this message nodes s0, . . . , s3 (knowing keyk10) compute H(k10) and XOR's with Ks0,...,s3 to get new group key GK0 (i.e., GK0← Ks0,...,s3 ⊕ H(k10)). Similarly messages sent by central node to existing group members areKs8,...,s11 ←H(k12) ⊕ GK0, Ks12,...,s15 ←H(k13) 747 747 746 746 746⊕ GK0, Ks4 ← H(k0) ⊕ GK0 and Ks7 ← H(k3) ⊕ GK0.

The nodes will compute the new group key GK0 by XORing received message with the hash of the keys known to them. Group key GK0 computed by nodes s8, . . . , s11 is GK0← Ks8,...,s11 ⊕ H(k12), for nodes s12, . . . , s15 it is GK0← Ks12,...,s15 ⊕ H(k13), for node s4 GK0← Ks4⊕ H(k0) and GK0 computed by node s7 is GK0← Ks7⊕ H(k3). The keys that are known to compromised nodes s5 and s6 are k1, k11 (keys with s5), k2, k11 (keys with s6). So by this the keys which are known to compromised nodes will not be shared to any of the available nodes in the network as sent by the central node, the keys in the central node message are encrypted by hash function. So with the help of the keys of the nodes which are compromised it is just impossible extract any information of the other existing nodes or of new group keys. Two different operations are being performed in order to prevent the attacks. Firstly new auxiliary is being generated by the nodes at the exit point of the network as per F (auxiliary key, new group key) ←− (Auxiliary key) XOR (New Group key). In the second step the hash values of the encrypted keys are just increased by one. No encryption method is being taken so as to communicate with the new group in the network and the hash values are taken and XOR operation is considered by which the overall communication overhead will be reduced i.e., rekeying cost is reduced.

Further for optimizing this technique, we will employ optimization i.e. using a Particle Swarm Optimization (PSO) algorithm.

Particle Swarm Optimization

Kennedy and Eberhart [28] introduced the Particle swarm optimization (PSO) algorithm which is an exploratory universal optimization technique that is grounded on swarm intelligence. The algorithm originates from the bird and fish flock movement behavior and is extensively utilized and quickly improved for the effortless application and necessitates fewer number of particles to be altered. By considering each key as a particle, it is possible to optimize the keys for encryption. PSO algorithm selects the key based on key connectivity constraint. Multiple key selection can be done by this process which provides user with the advantage of selecting nodes based on users requirement. By using optimized key selection process, key management can be improved for each sensor nodes.

The co-ordinate of every particle signifies a potential answer connected with two vectors i.e. the position vector and the velocity vector. Consider the n-dimensional optimization problem

Min f(x), where f: Rn □R
Consistent with every practical answer, the position vector is denoted by
xi= (xi1, xi2, xi3....., xin) and velocity vector is denoted by
vi= (vi1, vi2, vi3…., vin)

A swarm comprises of numerous particles which are contemplated to be the practical solutions that progress through the search space to obtain the ideal solution. All the particles must apprise their location on the basis of self-exploration, overall optimum swarm exploration and its earlier velocity vector consistent with the subsequent equations:

$$v_i^{k+1}=v_i^k+c_1r_1(pbest_i^k - x_i^k) + c_2r_2(pbest^k - x_i^k) \quad (1)$$

$$x_i^{k+1}= x_i^k + v_i^{k+1} \quad (2)$$

Where c1 and c2 are two positive constants called acceleration coefficients, r1 and r2 are random numbers, uniformly distributed in [0, 1].

$x_i = (x_{i1},x_{i2},x_{i3}.....,x_{in})$ is the present location of the ith particle.

$pbest_i = (x_{i1}^{pbest}, x_{i2}^{pbest}, x_{i3}^{pbest}... x_{in}^{pbest})$ is the position of the ith particle attained on the basis of its own experience.

$gbest_i = (x_{i1}^{gbest}, x_{i2}^{gbest}, x_{i3}^{gbest}... x_{in}^{gbest})$ is the location of the optimum particle on the basis of the overall swarms experience and k is the iteration counter.

A constant, maximum velocity (Vmax) is used to randomly restrain the velocities of the particle and advance the resolution of the search. However, to improve the exploration process, it is required to decrease the position of Vmax, and conceivably remove it completely, and an addition of an inertia weight w is done. The subsequent velocity update equation will be:

$$V_{id}^{t+1} = WV_{id}^{t} + C_1 r_1 (P_{id}^{t} - X_{id}^{t}) + C_2 r_2 (P_{id}^{t} - X_{gd}^{t}) \quad (3)$$

The PSO algorithm is depicted as:

For t = 1 to the max. Bound of the no. of iterations,

For i = 1 to the swarm size.

For j = 1 to the problem dimensionality.

Apply the velocity update equation (1)

Update position using equation (2)

End-for-j;

Compute fitness of updated position;

If needed, update historical information for p_{best} & g_{best};

End-for-i;

Terminate if g_{best} *meets problem requirements;*

End-for-t;

End algorithm.

VI. Result Analysis

For the enactment of this proposed method, the outcomes of this work is equated with previous work. The results justify that the proposed method aids in robust the security on sensor network when communicate. Hence the proposed methodology has maximum security and less overhead with effective key management. The evaluation of previous methods [12] [13] [14] and proposed solution based on below factors is described in table 1.

Parameters	Existing Approach(s)	Proposed Approach
Security	High	High
Computational Overhead	High	Low
Fine grain Access Control	Average	High
Collision Resistant	Average	Low
Key Size	Linear	Constant
Memory occupancy	High	Medium

Table.1 Comparative Analysis

VII. Conclusion

In this paper, the framework offer a secure mechanism and effective key management over data such as generation, distribution etc. in WSN with minimum overhead. A hash tree based key management scheme is used

to compute the new group key and distribute to group members efficiently in terms of storage, communication and computation. The proposed work can be further elongated to more secure and reliable in the aspect of data and energy respectively.

References

[1] A W. Heinzelman, A. Chandrakasan, And H. Balakrishnan, "Energy Efficient Communication Protocol For Wireless Microsensor Networks," In: Proceedings Of The 33rd Annual Hawaii Int'l Conf. On System Sciences. Maui: Ieee Computer Society, Pp.3005−3014, 2000.

[2] A.Manjeshwar And D. Grawal, "Teen: A Protocol For Enhanced Efficiency In Wireless Sensor Networks," In: Proceedings Of The 15th Parallel And Distributed Processing Symp. San Francisco, Ca: Ieee Computer Society, Pp.2009−2015, 2001.

[3] K. Romer And F. Mattern, "The Design Space Of Wireless Sensor Networks," Ieee Wireless Communications, Pp.54–61, 1999.

[4] X. Cao And G. Chen, "Ross: Resource Oriented Security Solution For Heterogeneous Clustered Sensor Networks," Int. J. Of Intelligent Control And Systems, Pp. 317- 324, 2007.

[5] H. W. Chan, A. Perrig, And D. Song, "Random Key Pre-Distribution Schemes For Sensor Networks," In: Proceedings Of Ieee Symp. On Security And Privacy, Pp.197-215, Berkeley, Ca, 2003.

[6] L. Eschenauer, Virgil.D Gligor, "A Key Management Scheme For Distributed Sensor Networks," In: Proceedings Of The 9th Acm Conference On Computer And Communication Security, Washington Dc, 2002.

[7] Q. Gu, And J. Drissi, Localized Broadcast Authentication In Large Sensor Networks, Int. J. Of Intelligent Control And Systems, Pp.341- 350, 2007.

[8] B. Lai, S. Kim, And I. Verbauwhede, "Scalable Session Key Construction Protocol For Wireless Sensor Networks," Ieee Workshop On Large Scale Real-Time And Embedded Systems (Lartes), Austin, Tx, 2002.

[9] C. Zhang, M. C. Zhou, And M. Yu, "Ad Hoc Network Routing And Security: A Review," International Journal Of Communication Systems, Pp.909-925, 2007.

[10] W. Abdallah, N. Boudriga, D. Kim, And S. An, "An Efficient And Scalable Key Management Mechanism For Wireless Sensor Networks," Icact Transactions On Advanced Communications Technology (Tact) Vol. 3, Issue 4, July 2014.

[11] L. Shen And X. Shi, "A Dynamic Cluster-Based Key Management Protocol In Wireless Sensor Networks, International Journal Of Intelligent Control And Systems, Vol. 13, No. 2, June 2008.

[12] M. Munther A. Majeed, Khalid A.S. Al-Khateeb, Mohamed R. Wahiddin And Magdy M. Saeb, "Protocol Of Secure Key Distribution Using Hash Functions And Quantum Authenticated Channels (Kdp-6dp)," Journal Of Computer Science Pp.1123-1129, 2010.

[13] M. Wen, Z. Yin, Y. Long, Y. Wang, "An Adaptive Key Management Framework For The Wireless Mesh And Sensor Networks," Wireless Sensor Network, Pp.689-697, 2010.

[14] A. Wadaa, S. Olariu, L. Wilson, M. Eltoweissy, "Scalable Cryptographic Key Management In Wireless Sensor Networks," Proceedings Of The 24th International Conference On Distributed Computing Systems Workshops, 2004.

[15] Y. Qian, K. Lu, B. Rong, H. Zhu, "Optimal Key Management For Secure And Survivable Heterogeneous Wireless Sensor Networks," Ieee Communications Society Subject Matter Experts For Publication In The Ieee Globecom 2007 Proceedings, 2007.

[16] A. Perrig, R. Szewczyk, V. Wen, D. Cullar And J.D. Tygar, "Spins: Security Protocols For Sensor Networks," In Proceedings Of The 7th Annual Acm/Ieee International Conference On Mobile Computing And Networking (Mobicom),Rome, Italy, Pp.189-199, July 2001.

[17] Y. Liu, S.K. Das And A. Chandha, "Group Key Distribution Via Local Collaboration In Wireless Sensor Networks," In Ieee International Conference On Sensor And Adhoc Communications And Networks (Secon), 2006.

[18] D. M. Wallner, E. J. Harder, R. C. Agee, "Key Management For Multicast: Issues And Architectures," Informational Rfc, Draft-Wallner-Key-Archootxt, July 1997.

[19] H. Harney, C. Muckenhirn, "Group Key Management Protocol (Gkmp) Architecture", Rfc 2094, July 1997.

[20] H. Harney, C. Muckenhirn, "Group Key Management Protocol (Gkmp) Specifications," Rfc 2093, July 1997.

[21] D. Mcgrew And A. Sherman, "Key Establishment In Large Dynamic Groups Using One Way Function Trees," May 1998.

[22] A. Perrig, D. Song And J. Tygar, "Elk: A New Protocol For Efficient Large-Group Key Distribution," In Proceedings Of The 2001 Ieee Symposium On Security And Privacy, 2001.

[23] A. K. Wong, M. Gouda, And S. S. Lam, "Secure Group Communication Using Key Graphs," Proceedings Of Acmsigcomm, Vancouver, British Columbia, September 1998.

[24] A. Kandlur, D. Pendarakis, Chang, R. Engel And D. Daha, "Key Management For Secure Internet Multi-Cast Using Boolean Function Minimization Technique," Acm Sigcomm'99, March 1999.

[25] R. Rivest, "The Md5 Message-Digest Algorithm. Rfc 1321, April 1992.

[26] R.L. Rivest, A. Shamir, And L.M. Adleman, "A Method For Obtaining Digital Signatures And Public-Key Cryptosystems," Communications Of The Acm, Vol.21, No.2, Pp.120-126, 1978.

[27] W. Zhang And G. Cao, "Group Rekeying For filtering False Data In Sensor Networks: A Pre-Distribution And Local Collaboration Based Approach," In Infocom Ieee, Pp. 503-514, 2005.

[28] J. Kennedy, And R. Eberhart, "Particle Swarm Optimization," Proceedings Ieee International Conference Neural Networks, 4, 1995.