AN ENERGY EFFICIENT KEY MANAGEMENT SCHEME FOR MOBILE WIRELESS SENSOR NETWORKS

[1]Dr. C.Gnana Kousalya, [2]Dr.T.Sasilatha, [3]M.Senthil Murugan

[1]Professor & Head , Department of ECE, St.Joseph's Institute of Technology, (India)

[2]Vice Principal, S.A. Engineering College, (India)

[3]Associate Professor, Department of ECE, St.Joseph's Institute of Technology, (India)

ABSTRACT

In Wireless Sensor Networks (WSNs), a sensor node communicates with a small set of neighbour sensor nodes and with the base station through a group leader or a cluster head. However, in some occasions a sensor node required to move in the sensor networks. The node has to change its own position with the requirement of applications. Considering this phenomena in this paper we propose to design an angular function and private key management system by group leader for the transmission of a node. In the proposed scheme, the group is divided into sectors. The motion of the node is related with the angles to the group leader and it is the basis of our proposal. The wireless sensor network divided into groups the nodes movement and activity should be tracked. The proposed scheme attains high connectivity and security with the help of the directional trans - receiver. The lifetime of a node is increased and it enables a node to move through the network and to transmit data to its neighbors.

Keywords: Wireless Sensor Network, Group Leader, Cosine Function, Angular Movement.

I INTRODUCTION

1.1 Wireless Sensor Networks (WSNs)

Ubiquitous computing can be implemented by considering Wireless Sensor Networks (WSNs) as a foundation network. [1] Wireless network with a collection of ultra light and low power sensors is termed as a wireless sensor network. Each sensor is equipped with limited resources such as memory and processor. [2, 3] After the distribution of nodes, they gather data from surroundings; [4] the data may take many forms such as temperature, sound or traffic. The gathered data is transmitted to the central base station or to the sink. [5] WSN has wide range of applications in every field like scientific exploration in civil operations, battlefield surveillance in military, security monitoring, target tracking and in health care system. [6]

1.2 Threats to WSN

In sensor networks, the major network layer attacks include spoofing, altering, or replaying routing information, sinkhole attacks, Sybil attacks, wormholes, HELLO flood attacks, Acknowledgement spoofing and node Capture

Attacks [7] At routing protocol, the attacker aimed to alter the routing information transmitted between nodes, this kind of attack is termed as direct attack. Through this, adversaries can repel the network traffic, lengthen or shorten the source routes, transmit false error messages, generate routing loops, divide the network and increase end-to-end delay. [8].Some messages are repudiate or dropped by adversaries in selective forwarding attack. In addition, an adversary assures that they do not transmit any further. In simple, it behaves as a black hole and it refuse to forward any packet it receives. [9] In case of sink hole attack, network traffic is trapped by the attacker in particular area. This process is being done by adversary through a compromised node; it creates a sinkhole at the center. [10]

In Sybil attack, the compromised node generates and broadcasts multiple identities in the network. This attack gradually lessens the effectiveness of network fault tolerant level in terms of topology maintenance, distributed storage and inconsistency. In the event of wormhole attack, messages received at one part are tunneled over a low quality link and reiterated in some other part. [11]

1.3 Issues of Key Management Schemes in WSN

Since, sensor nodes under go with limited energy constraint, energy efficiency is an important design goal of communication protocol. This design goal is also applicable for designing security schemes in WSN. [12] Therefore, a security service must consider energy efficiency as a performance metric. The level of security varies from one application to another and it generally relies on significance of information being transmitted. [13] When sensitive information is transmitted between nodes, a secure communication tunnel became an essential for the applications. [14]

Generally, in WSN, implicit or explicit link layer acknowledgements are considered in many routing algorithms. However, owing to broadcast medium of sensor network, it is possible to overhear and spoof the ACK packets transmitted in link layer by an adversary. In this circumstance, the objective of attacker is to compromise the sender by making believe that a weak link is strong and a disabled node is alive. Thus, the compromised node transmits data packets through the weak or dead link and paves way for an adversary to initiate a selective forwarding attack. By this attack, the destination node is also convinced by an adversary to forward packets on weak or less quality links. [15]

The malicious user seizes, corrupts and takes control over the node by utilizing the combination of passive, active and physical attacks. The attack of achieving control over a node is known as “Node Capture Attack”. The main causes of this attack are improper consideration of sensor nodes and cost constraint (high cost) of foolproof hardware, which can be implemented in portable devices. The attacks that are reasoned by compromised nodes have impact that is more negative in the network than the attacks from outside the network. It is difficult to keep an eye on nodes, since, nodes have freedom to join and leave the network at any time. In keying scheme, after the nodes are compromised, the keys are disclosure to the intruders. The attacker makes use of this complicated situation to compromise other node keys in the network. Finally, the entire network is spoiled by the attacker. [16]

1.4 Problem Identification

The scheme proposed in [18] is an energy efficient key management scheme, but it does not describe about the condition when a node moves from one group to another group or another node wants to join in the network. As an extension to this work, we focus on two types of keying technology; at first we present a shared key for neighbor detection and the second method shows mobility of the nodes in the network with the introduction of the group head and grouping of nodes. The joining concept given by Jinsu Kim et al. [1] gives a clear idea about the introduction of a new node in a given group and its authentication through the group head. However, it does not give crystal clear technique for the traverse of a node from group to another group. For that, we have designed a solution, which divides the groups into sectors and from a cosine angular key management system. It is more secure and directional.

The paper is organized as follows. Section 2 gives a brief literature review on various key management schemes for WSN. Section 3 describes proposed key management scheme. Section 4 describes the performance evaluation. Section 5 concludes the paper.

II Related Works

2.1 A Routing-Driven Key Management Scheme for Heterogeneous Sensor Networks [19]

The author presented an efficient Elliptic Curve Cryptography ECC-based key management scheme for heterogeneous sensor networks. The scheme utilizes the fact that a sensor only communicates with a small portion of its neighbours and thus greatly reduces communication and computation overheads of key setup. Their ECC-based key management scheme only pre-loads a small number of keys in each sensor and significantly reduces sensor storage requirement. The performance evaluation and security analysis demonstrated that the ECC-based key management scheme could significantly reduce sensor storage requirement and energy consumption while achieving better security (e.g., stronger resilience against node compromise attack)

2.2 Energy Efficient Key Management Protocol in Wireless Sensor Networks [1]

If a new node authenticated by reliable BS is added to a group through the move or insertion of the node, it results in the occurrence of unnecessary data transmission including the exchange of a large volume of information for generating a shared key with neighbour nodes, so such unnecessary data transmission should be minimized. The channel is elected and sensed information is transmitted through stable information exchange by applying an existing key management method to the group-based routing protocol, but when a new node is added or existing nodes are assigned mobility, the existing key management method has a limitation. A group-based key management method that can set a shared key faster and more securely using a multiple-key ring assigned to each node before deployment in-group formation within WSN. This key management method showed that it could work more energy-more efficient than existing key management methods even when nodes are mobile or new nodes are inserted.

2.3 A New Key Establishment Scheme for Wireless Sensor Networks [17]

Key establishment scheme can achieve quick authenticity without extra computations and communications. Tree-based key exchange protocol with LU Matrix Composition (TKLU) has three protocols, which are pair wise key

establishment protocol, Path Key establishment protocol and group key establishment protocol. Sensor nodes who are neighboring can establish pair wise key after they are deployed by LU composition technique. In addition, they are able to authenticate each other in the process of pair wise key establishment. Sensor nodes who are not neighboring should establish secret keys over the multi-hop path. They can achieve to agree on keys in insecure channel. Even if the third parties obtain the message, they cannot deduce the keys. It also can achieve authenticity at the same time. Those neighborhood nodes can agree on group key for secure data aggregation.

III PROPOSED SOLUTION

3.1 Assumptions

The network is divided into groups. The group can be of any size and any type. The group has a group leader. The nodes in a group have directional trans-receivers and the number of trans-receiver is equal to the number of arms in the group. A part of a group is related to a part of another neighbor group. A switching device is deployed at the group head, which is used to select the direction of transmission. When a node is moving from one group to another group it can carry a cosine angular function with it. Every Node in the wireless system has GPS system/transmitters. The group head keeps a track of the nodes present in the groups. Group leader (GL) can communicate with each other. When the node is moving from its coverage area it gives an angular function to the moving nodes. All nodes should have a common key with group leader for sending information from other nodes in the same group or for receiving a query from GL. This key is called the private key. The private key is generated and assigned before nodes are deployed. That is, the unique key (K_l^m) of each node (l) is generated by GL using $gk_i = f_k(l)$, where f is a pseudo-random function, and K^m is the master key known only to the controller at group leader. Different group should have different private key. The key generating function should vary for the groups. Because of the efficient computing ability of the pseudo-random function, the overhead caused by private key generation is negligible. The nodes are able to communicate with each other with a shared key. Nodes can communicate with the group head with the private key. Group head keeps the data of the private keys of all the nodes in the work. A node can be registered with one group in a time period. For finding the angular value all the groups in a region have to take a single direction for references. A joining concept is given in [1] is being added by us to solve this problem. A GL can only transfer the data only to the neighbour GLs. The data packet type or the used frequency should vary from node to node transmission and GL to GL transmission. Without shared key no node is able to get the data from the other node. When a node moves from a certain group all the nodes in contact with the travelling node should erase the related shared keys of the travelling node in them. A node is able to communicate with their neighbour node if they are in the same group.

3.2 Shared Key Systems

The proposed Key management scheme [18] is based on the state of sensor nodes. State of sensor nodes are categorized into three types as follows: Current transmitting node (CTN), Transmitting node (TN), none transmitting

Node (NTN). In The proposed scheme RTS/CTS control frames is slightly modified from their original MAC protocol (Figure 1) for informing a node the fact that its state is changed to TN or NTN in the corresponding period.

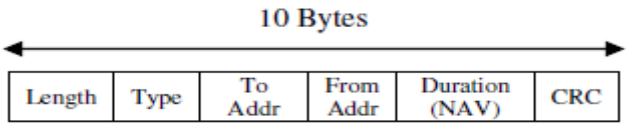

Figure 1a: The Original RTS and CTS Frames

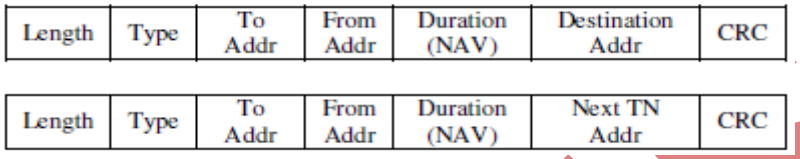

Figure 1b: The Modified RTS and CTS Frames

The modified RTS and CTS frame adds only one field of two bytes to the original frame. The newly added bytes in the RTS are the destination address and the newly added bits of CTS are TN address.

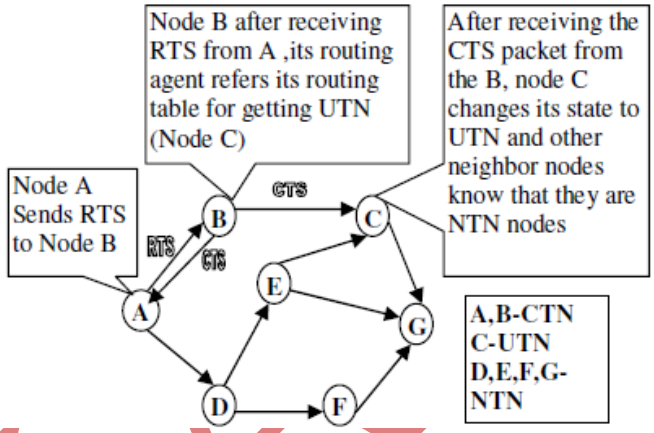

Figure 2: Classification of Node States

Figure 2 shows the classification of node states. When node B receives A's modified RTS frame including the destination address of the sink, its routing agent refers to the routing table for getting the next TN (node C) and informs back to its MAC. The node B then transmits modified CTS frame to node C, which changes its state to TN and other. An Energy-Efficient and Resilient Traffic-Aware Key Management Scheme for Wireless Sensor Networks neighbour nodes become aware of the fact that they are NTN nodes.

3.3 Network Architecture

Every group contains six directional trans- receivers. At the joining point of area of six directional trans-receivers the group head is present. Each trans-receiver is responsible for the connection of another neighbour group present in the network. The five ranges of trans-mission are 1^0-60^0, 61^0-120^0, 121^0-180^0, 181^0-240^0, 241^0-300^0, 301-$360^0/0^0$. Here the east point is taken as reference that is 0^0. In the above example the central group is A, Here C is communicating with A within the angle of 120^0 to 180^0. A is communicating with C in angles between 300^0 and 360^0. The difference between the angles is 180^0.

3.4 Data Structures and Tables

To keep the track of the movement of nodes; the group head keeps a table so that it can manage the security as well as assign a sacred function. The table enables a node to travel to a different group and a checking facility for the group head to avoid the interference of other unwanted node in a given group region. The table structure is given below

Table-1 Table stored at the group head

<Node id>	Angle with the reference point through which the node is moving to another group	Angular cosine function multiplied with the private key	Is node passed the coverage area (yes/no)	Received cosine function multiplied with the private key	Summation of both functions
……..	……..	……	……	……	…….

When the group head refers to another group head for the authentication the group head generates a data packet. The detail of the data packet is given below

Table-2 Data packet format at the group heads

<Node id>	Private Key multiplied angular cosine function

After getting this type of data packet the group head of another group sends an acknowledgement.

3.5 Shared key procedure:

For the formation of secure key we have used some cosine function

(i) When a node wants to communicate with the neighbour node it first gets the position of the neighbour node with the help of a GPS / transmitter.

(ii) The interested node will send a request to the group head for communication with the other node.

(iii) The node requests using the node id

(iv) The group head checks whether it comes in its authentication criteria. If it is there in the authentication area then it sends permission to both the nodes require a connection.

(v) Both the node shares their information using the shared key. The shared key can be generated by using the methods given in [18] [7] [17].

Phase-1

The node sends a request to the group leader for authentication of sharing of data with node 2.

Phase-2

After getting requests from node 1 GL checks its availability in it and sends permission to both the nodes.

Phase-3

The two nodes are communicating using the sharing key. The sharing key methods are given in [18] [7] [17].

3.6 Group Authentication Procedure

In our designed angular secure key management system, we are following the following steps-

The group leader (GL1) gives a private key to each node presents in its coverage group. Using the private key any node can transfer data with the group leader.Group leaders keep a register of the node IDs and assigned private keys.Here groups G1 and G2 are two neighbours. The GL1 is the group leader of G1 and GL2 is the group leader of G2.When a node is moving from its group area to another group leader (GL2) area the GL1 tracks the angle. It can be easily obtained as GPS system is deployed.

IV PERFORMANCE EVALUATION

4.1 Simulation Parameters

The key pool size K is a critical parameter because in random key distribution schemes the amount of storage reserved for keys in each node is likely to be a preset constraint, which makes the size of the key ring R a fixed parameter. Once R is set, then for larger values of K the probability that two nodes will share a key is small. The proposed Energy Efficient Key Management (EEKM) technique is evaluated through NS-2 [19] simulation. We consider a random network of sensor nodes deployed in an area of 500 X 500m. The number of nodes is fixed as 100 and the speed of the each node is fixed as 10m/s. The simulated traffic is CBR with UDP. The number of groups formed is 9. Out of which, we transmit data from 4 group heads to the sink. Three sensor nodes in each group are sending data to their group head.

4.2 Performance Metrics

The performance of EEM technique is compared with the Traffic Aware Key Management TKM [18] scheme. The performance is evaluated mainly, according to the following metrics.

- **Energy**: It is the average energy consumed for the data transmission.
- **Fraction of Communications Compromised:** Here we are going to calculate how a node capture affects the rest of network resilience. It is calculated by estimating the fraction of communications compromised between non compromised nodes by captured nodes
- **Average Packet Delivery Ratio:** It is the ratio of the number of packets received successfully and the total number of packets transmitted.

4.3 Results and Analysis

Keeping the number of nodes as 100, the number of compromised nodes is varied as 5,10,15,20 and 25.

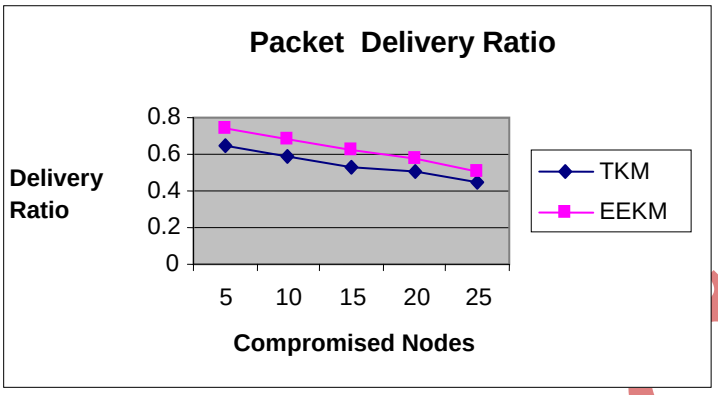

Figure-3 Packet Delivery Ratio Vs Compromised Nodes

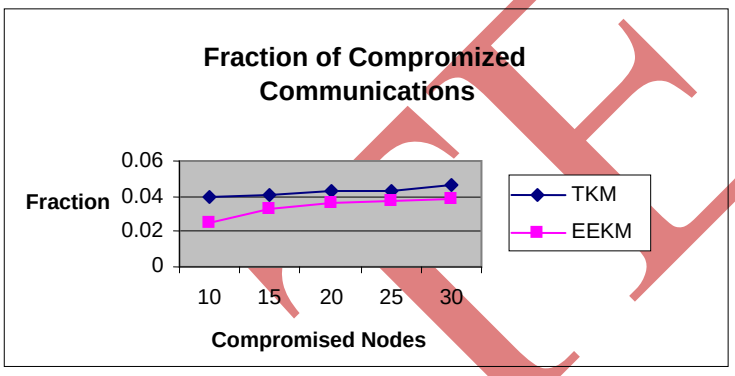

Figure-4 Fraction of Compromised Communications Vs Compromised Nodes

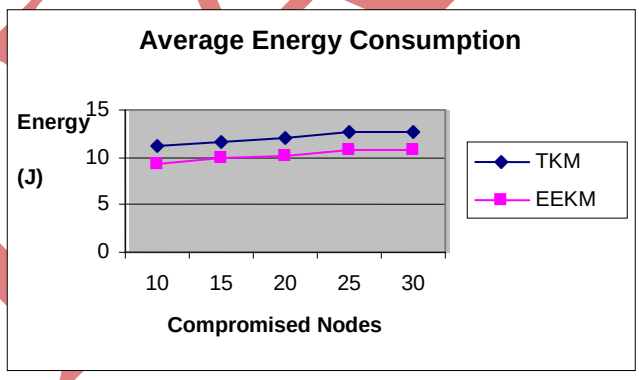

Figure-5 Energy Consumption Vs Compromised Nodes

Fig. 3 shows the packet delivery ratio of both EEKM and TKM techniques. When the compromised nodes are increased, naturally the packet drop will increase and hence the packet delivery ratio will be decreasing. From the figure, we can observe that EEKM has 13% higher packet delivery ratio, when compared to TKM.

Fig. 4 presents the fraction of communication compromised against node capture for both the techniques. When the number of compromised nodes is increased, the impact of attack will be more resulting in the increase of fraction of

compromised communications. But as it can be seen from the figure, the compromised fraction for EEKM is 16% less when compared to TKM.

Fig. 5 shows the average energy consumption of both the techniques. From the figure, it can be seen that the average energy consumption increases, when the number of compromised nodes is increased. This is due to the reason that when compromised nodes are increased in the network, more key updates takes place, thus consuming more energy. From the figure, it is evident that EEKM consumes 15% less energy than TKM.

V CONCLUSION AND FUTURE WORK

In this paper, we have proposed an angular movement aware key management scheme for wireless sensor networks. The proposed scheme is based on the movement of the node in wireless sensor network and passed through an authentication stage. Our scheme establishes secure key for active sensor nodes, which participate in direct communication and moves freely anywhere in the wireless sensor network. In this scheme, without disturbing ongoing security process movement of sensor node among different group is enabled. The proposed scheme attains high connectivity, which can be shown through numerical results. Simulation results show that the proposed scheme with angular function achieves stronger resilience, low energy consumption and increased delivery ratio when compared with the existing scheme. For future research we propose extending this security framework to include trust establishment and trust management in sensor networks. Besides this, we have an interest in exploring and solving security issues in multimedia and biometric security, cyber security and information assurance, protection against identity theft, and forensic computing.

REFERENCES

[1] Jinsu Kim, Junghyun Lee, and Keewook Rim, "Energy Efficient Key Management Protocol in Wireless Sensor Networks", International Journal of Security and Its Applications, Vol. 4, No. 2, April, 2010

[2] Gaurav Jolly, Mustafa C. Kuşçu, Pallavi Kokate and Mohamed Younis, "A Low-Energy Key Management Protocol for Wireless Sensor Networks", In the Proceedings of the 8 th IEEE Symposium on Computers and Communications (ISCC'2003), 2003

[3] Firdous Kausar, Sajid Hussain, Laurence T. Yang and Ashraf Masood, "Scalable and efficient key management for heterogeneous sensor networks", The Journal of Supercomputing archive, Volume 45 Issue 1, pp- 44 – 65, July 2008

[4] Giacomo de Meulenaer, Franc¸ois Gosset, Franc¸ois-Xavier Standaert and Olivier Pereira, "On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks", IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, (WIMOB '08), pp- 580 – 585, 2008

[5] Jong-Myoung Kim, Joon-Sic Cho, Sung-Min Jung, and Tai-Myoung Chung, "An Energy-Efficient Dynamic Key Management in Wireless Sensor Networks", IEEE 9th International Conference on Advanced Communication Technology, pp- 2148 – 2153, 2007

[6] Rohith Singi Reddy, "key mangament in wireless sensor networks using a modified Blom scheme", Cornell University Library, Cryptography and Security, 2011

[7] Le Xuan Hung , Ngo Trong Canh, Sungyoung Lee , Young-Koo Lee and Heejo Lee, "An Energy-Efficient Secure Routing and Key Management Scheme for Mobile Sinks in Wireless Sensor Networks Using Deployment Knowledge", Sensors, pp-7753-7782, DOI: 10.3390/s8127753, 2008.

[8] Virendra Pal Singh, Sweta Jain and Jyoti Singhai, "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010

[9] Sun Dong-Mei and He Bing, "Review of Key Management Mechanisms in Wireless Sensor Networks", Acta Automatica Sinica, Vol. 32, No. 6,November, 2006

[10] D. Sheela, Nirmala. S, Sangita Nath and Dr. G Mahadevan, "A Recent Technique to Detect Sink Hole Attacks in WSN", International Conference Program Bangkok Thailand, (ISEM2011), July, 2011

[11] Tejpal Singh, Vinod Kumar, Khushboo Saxena and Akanksha Saxena, "Evaluation of Security Conditions of Protocols for Data Routing in Wireless Sensors Networks", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-1, Issue-1, March 2011

[12] Ju-Hyung Son, Jun-Sik Lee and Seung-Woo Seo, "Topological Key Hierarchy for Energy-Efficient Group Key Management in Wireless Sensor Networks", Springer, Wireless Personal Communications Volume 52, Number 2 (2010), 359-382, DOI: 10.1007/11277-008-9653-4

[13] Ismail Mansour, G´erard Chalhoub and Michel Misson, "Energy-Efficient Security Protocol for wireless Sensor Networks Using Frequency Hopping and Permutation Ciphering", Proceedings of the 1st International Conference on Pervasive and Embedded Computing and Communication Systems, pp- 277-282, March, 2011

[14] Chee-Yee Chong and Srikanta P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges", Proceedings of IEEE Magazine, pp- 1247 – 1256, 2003

[15] Hemanta Kumar Kalita and Avijit Kar, "Wireless Sensor Network Security Analysis", International Journal of Next-Generation Networks (IJNGN), Vol.1, No.1, December 2009

[16] Patrick Tague, Mingyan Li and Radha Poovendran, "Mitigation of Control Channel Jamming under Node Capture Attacks", IEEE Transactions on Mobile Computing, pp- 1221 – 1234, 2009

[17] Xiaojiang Du, Yang Xiao, Song Ci, Mohsen Guizani and Hsiao-Hwa Chen, "A Routing-Driven Key Management Scheme for Heterogeneous Sensor Networks", IEEE Transactions on Wireless Communications, Volume 8 Issue 3, pp- 1223-1229, March 2009

[18] C. Gnana Kousalya and G. S. Anandha Mala, "An Energy-Efficient and Resilient Traffic-Aware Key Management Scheme for Wireless Sensor Networks", European Journal of Scientific Research ISSN 1450-216X Vol.50 No.2, pp.246-262, 2011