ISSN:0975-9646

Location Based Group Key Generation in Wireless Sensor Network

Ambika.N[#1], G.T.Raju[*2]

[#] *Dept of MCA(VTU), Dayananda Sagar college of Engineering,*
Research Scholar, Bharathiar University, India
[*]*RNSIT*
Dean & Head of CS Dept, RNSIT
Bangalore, India

***Abstract*— Sensors provides flexibility to the user to be deployed in any environment of user's choice. In spite of many disadvantages, the beneficiary factors have provided a strong intention to use these nodes as a monitoring tool to ease human effort. To add better integrity to the data being transmitted, encryption key can be utilized. Authenticating the data enhances security to a larger extent. In this study the above concepts are being focused. The paper generates encryption key which not only provides integrity to the data being transmitted, but strongly authenticates the source of the generation of data. The model adopts forward and backward secrecy. The study maximizes the security against sinkhole, Sybil and wormhole attack.**

Keywords*— *prevention and detection technique, location- based group key generation, key management, security, integrity, authentication, neighbor authentication

I. INTRODUCTION

Employing the sensors [2] in different applications over years has made these tiny elements a conventional practice. These devices have become a significant component in many applications [1-2], [20-22]. The usage of these sensors include providing temporary solutions in conferences, underdeveloped or sparsely populated areas, to manage relief operations during disasters like earthquakes, tsunamis, floods etc. These nodes prove to ease human effort regardless of its limitations. One of the primary advantages of using these devices are they go unnoticed. These devices are being utilized for monitoring the environment, keeping track of objects and alerting the user on time.

The number of nodes deployed varies from one application to another. The variation depends on their usage and the security level they demand. These low cost devices [23],[25] are prone to failures, hence stipulate security measures to transmit data from one end to another. The above mentioned shortcomings prove to benefit the intruders to launch different kinds of attacks. Two major kinds of attacks which can be introduced by the intruder are-

- *External attack* where the intruders will be able to snoop on the data being transmitted from one cluster to another.
- *Internal attack* is where the intruders get a control over the nodes, its keying material, and stored code. These nodes are termed as compromised nodes. The same have proved to be much dangerous than former kind of attack. The adversaries controlling the set of nodes can introduce different kinds of attacks in the network. Hence the base station/ sink node will not be able to receive reliable data from the environment.

The paper is modeled to tackle second kind of attack. To safeguard the data from this attack the transmitted data is being encrypted. Using encryption provides integrity and confidentiality to the data against different kinds of attacks. If the source from which the data is been transmitted is transparent to the sink node, the integrity of data becomes more reliable. Authentication takes the next step to bring the above concept into reality. Location based keys can be generated which could signal the base station indirectly of the status of the nodes deployed. Multiple nodes behave as detectors, notifying the malicious activity of the compromised nodes. The above concepts are being shelled into a stronger scheme and are being implemented to provide protected model.

The main contributions of the work can be summarized as follows.

- The network consists of heterogeneous nodes (nodes possessing different capabilities).
- The helicopter is behaving as a base station in this study.
- Airborne deployment is being utilized to deploy the sensors in the required environment. All the nodes are randomly deployed in the form of groups.
- 2-3 nodes in the cluster are Waspmote which have the potential to calculate the position. One of the nodes among the Waspmote is assigned as a detector by the base station. The other nodes in the cluster are utilized to sense the environment and transmit the same.
- To obtain accurate location information GPS residing in the helicopter synchronizes with the satellite GPS system.
- The cluster head calculates the positional information of other neighboring cluster heads by using the signal of the received data. This information is utilized to generate group

encryption key and this key is distributed to other cluster members of the cluster.

- Each cluster has a detector assigned by the base station, which provides information about the cluster members.
- At time interval T, the readings are collected by the helicopter.
- The neighboring cluster head also behaves as detector monitoring the activity of neighboring cluster.
- The base station is final decision maker (to conclude whether a node is compromised or not).
- The paper utilizes multi-hop transmission of data to reduce energy consumption of the nodes.

The rest of the paper is being fragmented in to 7 sections. The succeeding segment enfolds all the notations used in the paper. Portion 3 of the paper assimilates the assumptions made in the work. Subdivision 4 describes the assumptions made while designing the model. Segment 5 encompasses the proposed model, its architecture and its working. Section 6 provides the testimony of the proposed work. Partition 7 provides a description of the dissection provided against Sinkhole attack, Sybil attack and wormhole attack. Segment 8 provides inference of the work suggested.

In this study, sensors are being addressed as nodes, elements, tiny devices. The base station is addressed as helicopter, sink node.

II. RELATED WORK

The author in [4] has designed the work consisting of 4 phases. In Phase I, a trusted authority (TA) generates the system parameters, and initializes sensor nodes by delivering ID-based keys to them through a secure channel. In Phase II, sensor nodes are deployed, and each node can get its location and location-based key under the assistance of mobile robots. In Phase III, mutual authentication between neighbouring nodes is provided, and each node can establish shared keys with all its legitimate neighbours. In Phase IV, immediate pairwise key is established.

[1] presents a simple location-aware deployment model, and develops two pairwise key pre-distribution schemes, a closest pairwise keys pre-distribution scheme and a location-based pairwise keys scheme using bivariate polynomials, by taking advantage of sensors' expected locations.

In [26] group key is collaboratively established by combining the keys of all authenticated members, which helps in maintaining the communication and computation transparency among the group members.

III. NOTATIONS USED

TABLE II
NOTATIONS USED IN THE PROPOSED MODEL

Notation	Meaning
N_I	I^{th} node in the network
N	Network
M_{ID}	Master key
U_{ID}	Unique key stored in the nodes (used to identify the nodes in the network)
LOC (CH_I)	Determined location of cluster head I
CH_I	I^{th} cluster head of C_I .
C_I	I^{th} cluster of the network
BS	Base station
GPS_S	GPS location calculated by the satellite
ERR_RATE	Standard error rate (fixed rate)
LB_GPS	Lower bound of the calculated location
UP_GPS	Upper bound of the calculated location
GKG	Group-key generation model
PKG	Location – based Pair-wise key generation model
GPS_H	GPS Location calculated by the base station
GPS_{CAL}	Calculated GPS location (by the cluster head) using the received signal strength of the acknowledgement
$\|\|$	Concatenation
S_I	Signal strength

IV. ASSUMPTIONS

The following assumptions are made in the proposed work-

- The base station is assumed to be trustworthy. The base station generates the master key and unique ID and embeds it into the nodes before deployment in the environment. These keys in combination are used to authenticate themselves with the base station.

- The nodes are assumed not to be under any kind attack till they form cluster.

- The Waspmote deployed is assumed to calculate accurate GPS position reading. It is believed to make minute errors when calculating the GPS location (within bounds) of neighboring cluster head position.

- The intruder is assumed to behave as an imposter of another node (sinkhole attack), can introduce Sybil attack and wormhole attack inside the network.

V. PROPOSED MODEL

A. System model

Two types of nodes are utilized in the proposed model.

- Waspmotes are utilized as cluster heads. These nodes are utilized to aggregate the data obtained from the cluster members and forward the same to the next hop/ sinknode.
- Tinynode 584 is used as the cluster members. These sensors sense the environment, encrypt the data and forward the same to the respective cluster heads.

B. Deployment of nodes in environment

The nodes are embedded with unique key U_{ID} and a master key M_{ID} before deployment. The nodes are deployed randomly by helicopter in groups. These nodes enter the setup state where the nodes configure and broadcast a HELLO message to the nodes in the network. The same is denoted in notation 1. Node N_I broadcasts HELLO message to the network N.

$$N_I \rightarrow N: HELLO \quad (1)$$

The nodes within the communication range R acknowledges to the message. In notation 2, node N_J is sending the acknowledgement ACK to node N_I.

$$N_J \rightarrow N_I: ACK \quad (2)$$

The nodes authenticate with each other using master key. The same is represented in the equation 3. A list of nodes in the cluster in maintained in each other's memory. To avoid collision, time division multiple access (TDMA) is utilized.

$$N_J \leftrightarrow N_I: M_{ID} \quad (3)$$

C. Storing the location details of the nodes deployed

After the formation of the cluster, the cluster head is chosen considering the energy it possesses. The cluster head authenticates itself with the base station using master key M_{ID} and unique id $U_{ID.}$ From equation 4, encrypted message using master key M_{ID} and unique key U_{ID} is communicated to the base station BS by the cluster head CH_I.

$$CH_I \rightarrow BS: ENCRYPT(M_{ID}, U_{ID}) \quad (4)$$

The helicopter posses a GPS device, which calculates the approximate position of the cluster head. This value is synchronized with the GPS reading of the satellite against the GPS calculated by the base station. The same is represented in the equation 5.

$$\mathbf{BS \rightarrow GPS\_CAL} \left| \mathbf{GPS_H \pm GPS_S} \right| \quad (5)$$

D. Generation of group location keys

The distance from one node to another is calculated using the following 3 techniques-

1) Received signal strength
2) Time of arrival of packets
3) Time difference of arrival

In this study, the proposed model utilizes 1st approach is adopted to calculate the approximate distance of the neighboring cluster head.

The cluster head CH_I sends a message to the neighboring cluster head, identifying itself. By utilizing the received signal strength (equation 6 & 7) of each other, the distance GPS_{CAL} is calculated.

$$CH_I \rightarrow CH_J: M_{ID} \quad (6)$$

$$CH_J \rightarrow CH_I: ACK \quad (7)$$

By utilizing the calculated approximate location of the neighboring cells (cluster head) group key is generated. The same is represented in equation 8.

$$GPS_{CAL} \rightarrow S_I(ACK) \quad (8)$$

The cluster head calculates the group key and distributes it to its cluster members. The cluster member in turn utilizes this key for encrypting sensed data to transmit. This concept is represented in equation 9.

$$\mathbf{G_{KEY} \rightarrow ENCRYPT\_KEY(LOC(CH_I)||LOC(CH_J)||LOC(CH_K))} \quad (9)$$

Wherever a new cluster head is elected in the cluster, the process is being repeated. This process makes neighboring cells aware of the new cluster head location and proceeds by changing the encryption key by reforming using the location of the new cluster head in the neighboring cell. The above scheme implements forward secrecy. The old encryption key is being erased, implementing backward secrecy.

E. Evaluation done by the base station

The base station calculates the GPS location of the cluster head against the reading obtained by the respective cluster head and its neighbors. The value obtained is cross-verified with the GPS location information stored in the base station and this value has to be within the bounds. Equation 10 represents the above concept.

$$\left| \mathbf{GPS_{CAL} \sim GPS\_CAL} \right| \leq \mathbf{ERR\_RATE} \quad (10)$$

The difference between the actual GPS and calculated GPS has to be less than or equal to standard value (ERR_RATE).

$$LB\_GPS \leq ERR\_RATE \leq UB\_GPS \quad (11)$$

VI. SECURITY ANALYSIS

The following scenarios are considered to evaluate the work.

A. If the cluster member is compromised-

The encryption key of one cluster differs from another, as each cluster is surrounded by multiple clusters. If the cluster member is compromised it shall uncover the encryption key being utilized. To safe guard the previous messages sent to the base station, the previous group key and other location information is deleted after the formation of new encryption key. This technique implements backward secrecy. As the cluster head changes from time to time, the group key also varies from time to time. The above concept implements forward secrecy.

A cluster member will either deny sending messages or sends too many messages. As each cluster member is given a slot to send the message to the respective cluster head, any deviation from the regular activity is monitored by the detector. The detector sends its report at regular intervals of time. Apart from the detector, the cluster head also monitors unusual activity of the cluster member. Any suspicious activity is notified to the base station. The base station compares the negative report obtained from the cluster head and detector. If the report remains the same, the base station concludes the node as compromised and instructs the network to exclude it from the network.

b. If the cluster head is compromised-

If the cluster head is compromised, it may engulf all the messages sent by all the cluster members or deny forwarding the message. Once the cluster head will not respond to the message sent by the neighboring cluster head, the group head is suspected to be malicious. When the node is controlled by any intruder, the main task of it would be to embezzle as many data as possible. It will either deny forwarding the data or misuse the data by tunneling the data to different location and replaying it. The detector in the cluster supervises the cluster head. It notifies the base station of any unusual activity of the cluster head. To uphold its decision, the surrounding cluster heads also send their report (in case the cluster head does not respond to its message). The cluster head will not be able to calculate appropriate group key. The base station concludes the cluster head as compromised and alerts other nodes of the network. Another node is chosen as the cluster head after obtaining the message from the base station.

c. If the detector is compromised

The detector of the cluster is being assigned the task to monitor the activities of the other cluster members and notify the same to the base station. If the detector is assumed to be compromised, it will either send too many messages or will deny sending message. If the base station does not receive timely message or does not receive any message at all, it temporarily assigns another node to play the role of the detector.

VII. SIMULATED RESULTS

Helicopter is made to fly 20m to 150 m from the ground. The close proximity between the nodes and the helicopter provides accurate value. Usually the helicopter travel speed ranges from 180km - 210 km per hour. For every 6m the readings are collected.

The work is simulated using NS2. Heterogeneous nodes are been dispersed uniformly distributed in the network of dimension 500m * 500m. Table 3 provides the implementation details. Totally 500 nodes are being deployed in the network. Cluster can contain 8-9 cluster members (of which one of them is cluster head). 28 groups of 9 cluster members and 31 groups of 8 cluster members are being deployed. The simulated results are compared with PKG [1] and GKG [24]. Table 4, provides the parameters considered during implementation and table 4, provides the simulated result.

TABLE Iv
PARAMETERS USED DURING SIMULATION

Description	**Quantity**
Dimension of the network	500m * 500 m
Total number of nodes in network	500
Distribution of nodes	Uniform
Total number of nodes dispersed in the network	(9 nodes * 28 groups) + (8 nodes * 31 groups)
Total Length of encryption key	(132*2) - (132*5) bits
Number of cluster members in the cluster	8-9
Number of neighbors surrounding a cluster	2-5
Number of hops considered	0-2 hops

A. *Energy Consumption*

Energy is one of the essential resources when the nodes are deployed in unattended harsh environment. To conserve energy the following steps are being considered-

- The nodes if not performing any activity go to sleep mode.
- Eliminating the compromised nodes from the network help in conserving energy to a larger extent.
- Mobile base station is utilized, where data has to traverse only few nodes to reach its destination.
- Multi-hop transmission of data is being utilized.

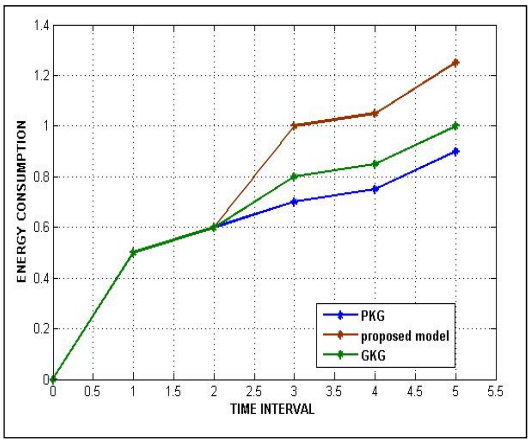

Fig. 1- Energy Consumption in PKG , PROPOSED MODEL AND GKG (assuming the network is not under any kind of attack)

The network utilizes two types of nodes, one being Waspmote and other TinyNode 584. The ratio of the nodes would be 1:3. The cluster containing 9 nodes inside the cluster contains 3 Waspmote and the cluster containing 8 nodes contains 2-3 Waspmote. The node near the boundary contains 3 Waspmote and the nodes away from the boundary line contain 2 nodes. The Waspmote have enough energy hence the cluster head will not fall short of energy to transmit or aggregate the data.

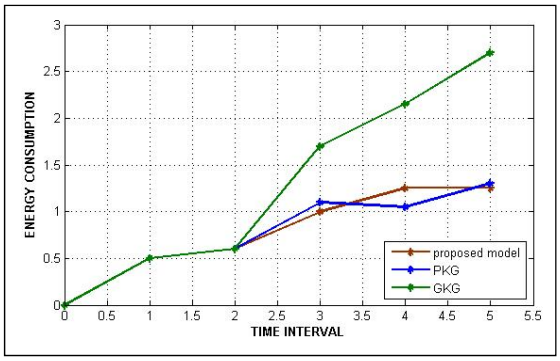

Fig. 2- Energy Consumption in PKG, PROPOSED MODEL AND GKG (Assuming the network is under sinkhole, Sybil and wormhole attack)

Though energy is one of the primary necessities to keep the network alive, the integrity of data has to be protected from the intruders. The transmitted data provides a picture of the unsupervised environment. The intruder can impart false alarm and necessity actions cannot be taken in time. Hence authentication and integrity of data provides a strong and reliable network. Fig .1, Depicts the energy consumed by PKG, GKG [24] and proposed model. The proposed model consumes 0.25% more energy than GKG model and 0.35% more energy than PKG model. Fig 2, Depicts the energy consumed in PKG, GKG and proposed model. The proposed model consumes 0.05% less energy than PKG model and 1.45% less energy than GKG model.

B. *Sybil Attack*

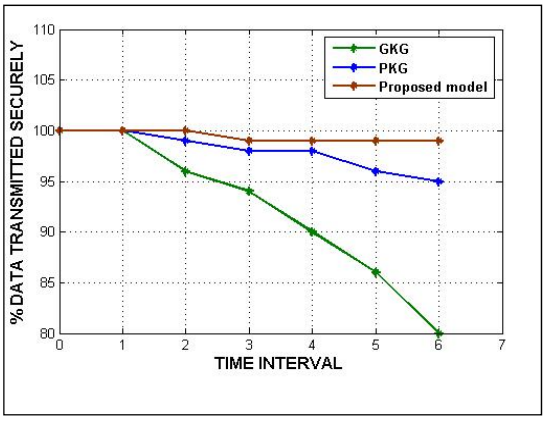

Fig. 3- Illustration of Sybil attack on GKG, PKG and proposed model

The nodes in network are liable to different kinds of attacks, among which Sybil attack [5-7] is one of them. The adversaries launching this kind of attack impersonate itself as one of the nodes among the nodes dispersed in the network. The adversary will get a hold on the concealed information stored in the nodes. Using this information, the adversary can manipulate the data and forward it to the base station. The base station will not be able to get accurate information hence will not be able to take appropriate action on time.

In this paper, the cluster head aggregates the data from the cluster members, which is being forwarded to the next hop or the base station.

The detector in the cluster monitors the activity of all the nodes in the cluster including the cluster head. Any abnormal activity is reported to the base station, which in turn takes appropriate steps to protect the network from malicious node. The base station calculates the accurate position of the cluster head using satellite. This data in turn is used as a cross-verification against the data collected from the cluster head (detect malicious node in the network under Sybil attack). From the fig 3, the proposed work secures data by 4% compared to PKG and 19% compared to GKG from Sybil attack.

C. *Sinkhole attack*

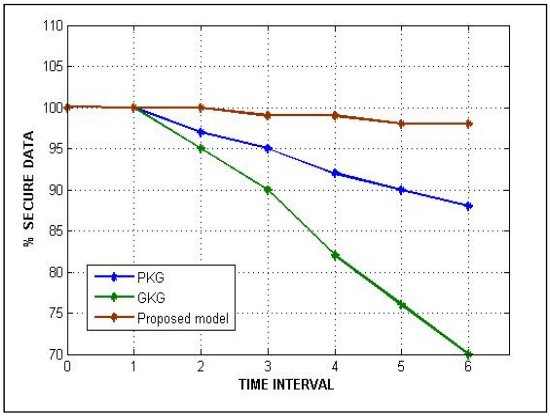

Fig. 4- Illustration of Sinkhole attack in PKG, GKG and proposed model

Sinkhole attack [13-17] is a kind of invasion to the nodes in the network where the intruder magnetizes the data packet towards itself. The nodes in their ignorance will not be able to recognize the intention of the node (controlled by the adversary) and hence will forward all its data.

In this paper, the cluster head and detector in the cluster monitors other cluster members of the cluster and reports the abnormal activity of the intruder/compromised node. Added to this, the paper uses mobile base station to forward its data. The cluster (cluster head acting as a detector) will be aware of its neighbour's status and data is being forwarded among the known nodes in the network. The proposed model takes care of the attack by protecting 10% of data compared to GKG model and 28% compared to PKG model from Sinkhole attack (fig 5).

D. *Wormhole attack*

Wormhole attack [8-12] is a damage intended to create by the intruder by tunneling the packets from one location to another and replaying the same. The base station unaware of the intention will not be able to depict a proper visualization of the environment and hence will be unable to take appropriate action on time.

In this paper, the cluster heads calculates the location where it is deployed and generates an appropriate location based group key with the help of the neighboring nodes. The position of the neighboring nodes guarantees the location information. Fig 5, depicts the result of wormhole attack. The proposed model provides 100% evaluation to the base station, if the nodes are invaded by the wormhole attack (intruders). The proposed model proves to provide 20% more reliability of data compared to GKG model.

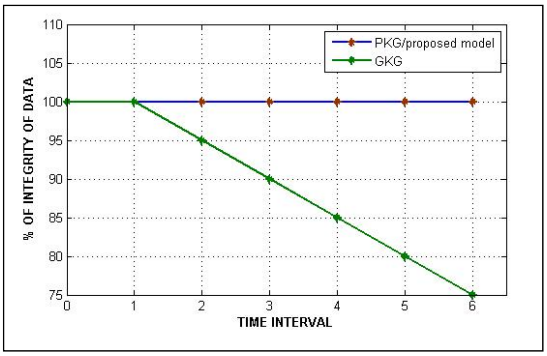

Fig. 5- Illustration of Wormhole attack in PKG, GKG and proposed model

TABLE V
SIMULATED RESULTS

Simulated result	**Proposed model**
Probability of detection of compromised nodes	>=0.9
Probability of data integrity	>=0.9
Probability of reliable data reaching base station	>=0.95
Threshold (after cross-verification of report obtained from detector, cluster head) considered to term a node as compromised	<=0.11

VIII. CONCLUSION

The paper considers mobile sink which moves from one end of the network to another collecting the sensed-encrypted data. To provide better authentication and integrity to the network, location based keys are generated. To provide robust authentication, the cluster utilizes location of neighboring nodes to generate the group key. This data is being cross-verified by the location data obtained by the satellite. This paper will be able to capture the compromised node and protect the rest of the nodes from Sybil, Sinkhole and Wormhole attack.

REFERENCES

[1] Donggang Liu ,Peng Ning, "Location-based pairwise key establishments for static sensor networks," in Proc. ACM SASN, Fairfax, VA, Oct. 2003, pp. 72–82.

[2] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE Comm. Magazine, Aug. 2002.

[3] D. Liu and P. Ning, "Location-Based Pairwise Key Establishments in Static Sensor Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2003.

[4] Mei-jiao Duan , Jing Xu, "An efficient location-based compromise-tolerant key management scheme for sensor networks" , Information processing letters, 2011.

[5] Kuo-Feng Ssu, Wei-Tong Wang, Wen-Chung Chang, Detecting Sybil attacks in Wireless Sensor Networks using neighboring information , The International Journal of Computer and Telecommunications Networking 2009, Volume 53 Issue 18 ; doi>10.1016/j.comnet.2009.07.013.

[6] James Newsome, Elaine Shi, Dawn Song, Adrian Perrig; The sybil attack in sensor networks: analysis & defenses, jan 2004.

[7] Ren Xiu-Li; Yang Wei , Method of Detecting the Sybil Attack Based on Ranging in Wireless Sensor Network , 5th International Conference on Wireless Communications, Networking and Mobile Computing,,2009, pg- 1-4,doi>10.1109/WICOM.2009.5302573.

[8] Yih-Chun Hu; Perrig, A.; Johnson, D.B.; "Wormhole attacks in wireless networks" , IEEE Journal on selected areas in commnication, volume 24, Issue 2, 370-380 , 2006 ; doi > 10.1109/JSAC.2005.861394.

[9] Zhibin Zhao; Bo Wei; Xiaomei Dong; Lan Yao; Fuxiang Gao; "Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis ", International Conference on Information Engineering (ICIE), 2010 , 251-254, doi> : 10.1109/ICIE.2010.66.

[10] Honglong Chen, Wei Lou, Xice Sun, Zhi Wang , "A secure localization approach against wormhole attacks using distance consistency", Journal EURASIP Journal on Wireless Communications and Networking - Special issue on wireless network algorithms, systems, and applications, Volume 2010, doi>10.1155/2010/627039.

[11] Modirkhazeni, A.; Aghamahmoodi, S.; Modirkhazeni, A.; Niknejad, N.," ", The 7th International Conference on Networked Computing (INC), 2011 , 122-128.

[12] Nabila Labraoui, Mourad Gueroui and Makhlouf Aliouat, Secure DVHop localization scheme against wormhole attacks in wireless sensor networks, European Transactions on Telecommunications, pg 303-316, 2011 DOI: 10.1002/ett.1532.

[13] Sharmila, S.; Umamaheswari, G., "Detection of Sinkhole Attack in Wireless Sensor Networks Using Message Digest Algorithms", International Conference on Process Automation,Control and Computing (PACC),2011,1-6;doi>10.1109/PACC.2011.5978973

[14] Krontiris, I.; Giannetsos, T.; Dimitriou, T.,"Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side" , IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2008. WIMOB '08, 526-531, doi > 10.1109/WiMob.2008.83

[15] Edith C. H. Ngai, Jiangchuan Liu, Michael R. Lyu , "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks", Journal Computer Communications ,2007, Volume 30 Issue 11-12; doi>10.1016/j.comcom.2007.04.025.

[16] Changlong Chen, Min song, George Hsieh, "Intrusion detection of Sinkhole attack in largescale wireless sensor network" , WCNIS 2010, Pg 711-716

[17] Ioannis Krontiris, Thanassis Giannetsos, Tassos Dimitriou, "Launching a Sinkhole Attack in Wireless Sensor Networks :The Intruder Side", WiMob 2008: pg - 526-531.

[18] G.J. Pottie and W.J. Kaiser, "Wireless Integrated Network Sensors," Comm. ACM, vol. 43, pp. 51-66, May 2000.

[19] C. Chong and S. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges," Proc. IEEE, vol. 91, no. 8, pp. 1247-1256, Aug. 2003.

[20] Hakala, I., Tikkakoski, M. ; Kivela, I. , "Wireless Sensor Network in Environmental Monitoring - Case Foxhouse" ,Second International Conference on Sensor Technologies and Applications, 2008", pg 202 - 208

[21] Zhuang, L.Q. , Goh, K.M. ; Zhang, J.B. "The wireless sensor networks for factory automation: Issues and challenges ", IEEE conference on Emerging Technologies and Factory Automation, 2007. ETFA. , pg 141-148.

[22] Gungor, V.C. , Hancke, G.P. "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches", IEEE Transactions on Industrial Electronics, Volume: 56, Issue: 10 , pg: 4258 - 4265 , 2009; doi > 10.1109/TIE.2009.2015754.

[23] Dezun Dong, Yunhao Liu and Xinbing Wang, " Edge self monitoring for wireless sensor network", IEEE transactions on parallel and distributed systems, vol. 22, no. 3, march 2011.

[24] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

[25] V. Giruka, M. Singhal, J. Royalty, and S. Varanasi, "Security in Wireless Sensor Networks," Wiley Wireless Comm. and Mobile Computing, vol. 8, pp. 1-24, 2008.

[26] Dhilak Damodaran, Rohit Singh, Phu Dung Le, "Group Key Management in Wireless Networks Using Session Keys", Proceedings of the Third International Conference on Information Technology: New Generations (ITNG'06).