ISSN:0975-9646

Linear Programming Model of Sensor Network

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

[#]*Research Scholar, Bharathiar university*
Coimbatore, India
[*]*Dean & Head of CS Dept, RNSIT*
Bangalore, India

***Abstract*— Sensors are tiny devices utilized as an essential component in many applications. These nodes are easing human effort by accomplishing task without any human intervention in areas including disaster relief, harsh environments. These devices are liable to get compromised as these nodes are unattended after deployment. Hence encryption keys are to be used to provide reliability to the data being transmitted.**

In this study,Different types of key management techniques and detection schemes are being considered to device the LP model. A Linear programming model is being developed to gauge the security in the network. To adhere to the concept, different constraints which directly influence security are being utilized. A key distribution technique is considered with the LP model architecture to check its effectiveness. This model can be used to estimate the strength of different input parameters in a environment against different kinds of attacks introduced by the adversaries. The study is goaled to enhance security against Sinkhole attack and Wormhole attack.

***Keywords*— Security model, Linear programming model, security estimation device, Sensor networks**.

I. INTRODUCTION

Wireless sensors [35] have become one of the significant domains which are being utilized widely in different applications. These sensors lessen the human effort by achieving the pre-assigned task in harsh/unsupervised environment. These nodes are application specific and hence their numbers vary from one application [1-2] to another. Some of the applications where these devices play an important role include military target tracking and surveillance [3-4], natural disaster relief [5] and biomedical health monitoring [6-7].Securing the network from various types of attacks becomes important as these nodes are not monitored.

Two major types of attacks are obvious, one being outside attack where the intruder will gain access on the message/data being transmitted and other being inside attack where the intruder gains access of the keys and other information stored inside the nodes and the nodes behavior is being controlled by the intruder. The intruder after gaining access of the nodes, can induce false data into the network, can deny forwarding the data, and can manipulate data. Hence inside attack proves to be more precarious leading to breach in integrity and authenticity.

To address such type of attacks, the nodes can be employed to adhere to some prevention techniques like key distribution and management. The nodes can fundamentally authenticate each other and then can utilize encryption keys to intensify its strength against different kinds of attacks. To increase the protection, detection mechanism can be employed which acquaints the network from the activities of compromised nodes.

To provide an optimal security in the environment the following questions are to be answered-

1. What is the objective of the protocol used?
2. If several parameters make up the objective, which should be given the highest priority?
3. What are the constraints on which these parameters depend on?

Linear programming provides a solution to the above problem. Linear programming is a mathematical method for determining a way to find the optimal solution from the feasible solutions available. The formula is generated focusing on the goal (objective function), its constraints and non-negative variables. Answers to the above questions are being quoted below.

The following parameters are being considered –

1. *Objective:* To provide maximum security to the network against different kinds of attacks introduced by the intruders.
2. *Constraints considered:*
   a. *Time slot:* The cluster head of the respective cluster provides a time slot to each of the cluster members to transmit its data.
   b. *Buffer size:* Considering huge amount of nodes which vary from 100-1000 in numbers, keeping a track of each one is a big task. Hence each cluster is monitored using a detector. Multiple detectors can be utilized to enhance security. The detector is used to monitor the size of the transmitted packets. If the number goes beyond the specified size, the node can be considered as compromised.

In literature, Linear programming are being utilized to minimize the energy, load scheduling, finding the appropriate path to the sink and so on. Formulating linear programming module to assess security is the first of this kind.

The paper is organized in the following manner. Section 2 contains the notations used in the study. Segment 3 gives a brief description of key management techniques and different detection proposals designed by different authors. Assumptions made in this paper are listed in section 4. System parameters, design of the proposal and its working are being detailed in section 5. The efficiency of any protocol is being measured as a sample in section 6. The paper is concluded in section 6.

II. NOTATIONS USED

Notation	Meaning
N_i	Cluster member of C_i cluster
C_j	i th cluster of the network
CH_i	Cluster head of C_i cluster
T_i	i the time at which data is being transmitted.
D_i	Detector of the C_i cluster
U_{ID}	Unique id stored in the cluster
E_i	Generated encryption key
T_p	The maximum length of the packet size of a node in the network
N_{total}	Total number of nodes in the network at the time of deployment
TH_i	Considered threshold (number of packets dispatched from one hop to another)
K	Total number of clusters in the network
S_{net}	Maximum number of nodes which are secure

TABLE I

III. BACKGROUND

Many key generation and management techniques have been designed by various authors. Some of them are being considered in this work.

Blom's method [20] is not built for key distribution. Many key generation techniques are built keeping this method as the base. This study considers two matrices, a symmetric table D of dimension (λ + 1)* (λ + 1) contains secret keys. This table is made private to the particular node. The second table G is any arbitrary table which is publicly available to all the nodes in the network. It has a dimension of (λ + 1) *n. the two communicating parties exchange the columns of public matrix, using the key is generated. Blundo method [21] is similar to Blom's method [20] with some variations. A random selection of t-degree symmetric polynomial is done.

Eschenauer and Gligor's method [22], key pool of random keys is generated using a key identifier. From this super set, subsets of keys are chosen with key identifier. This is known as key ring. The nodes before deployment are loaded with a key ring and the nodes willing to communicate tries to find a common key which is later used for encryption. The algorithm is designed such a way that only a single common key is present. This method is known as shared key discovery. To address the disadvantages of Eschenauer and Gligor's method, Q-composite key pre-distribution scheme [23] came up with some add-ins. This method has Q common keys to overcome path key establishment technique. To enhance security multipath key reinforcement scheme is proposed which creates a sequence of disjoint secure links.

Multiple space key pre-distribution scheme [24] is a combination of Eschenauer and Gligor's method and Blom's method. This method of key distribution enhances security against the other two mentioned methods [22], [20]. As in [20] a random matrix and symmetric matrices are being generated. The symmetric matrices generated vary in number. Using Blom's method a symmetric matrix is chosen to generate transpose matrix. Each instance generated is known as space. Using [22] the spaces, shared key and path key establishment procedure is done.

Polynomial pool based key pre-distribution scheme is a based on Eschenauer and Gligor's method and Blundo scheme of key distribution. A t-degree set F of bivariate symmetric polynomials is being constructed. A subset of polynomials is embedded in each sensor. To establish communication links, the nodes willing to setup secure link should posses at least one common polynomial. Using this polynomial shared key is calculated using Blundo scheme. If they don't have a common polynomial, they use path key establishment technique using Eschenauer and Gligor's method.

Two schemes are designed using combinatorial design based key pre-distribution scheme. Former one is where the key generation is based on [22] and is deterministically designed. A balanced incomplete block design is used to construct the key rings. BIBD scheme [25] works effectively when the number of sensors has to be prime power.

To overcome the limitations of [25] a hybrid scheme [26] was designed. If the number of sensors is not a prime power an alternate solution is suggested. The closest prime power is calculated to generate the key. Using this information shared key is established using [22].

A graphical representation of the network is assumed by considering sensor nodes as vertices and the communication link as edges. Using the connectivity property, expander graph is logically constructed. If an edge is found between two nodes, shared key is generated by the authority and assigned to the respective nodes before deployment. The keys vary from one to another. Expander graph-based key pre-distribution scheme [27], where shared key discovery process is avoided, but path key establishment is to be performed. A peer intermediate for key establishment [28] is based on mathematical structure. A two-dimensional grid is constructed by the authority keeping the sensors in particular location in the grid. All the nodes are provided with an identity depending on respective location in the grid. Depending on the edges between the nodes, shared key is assigned to the nodes with connectivity inside the grid.

Random assignment set selection key pre-distribution scheme [29] addresses the availability of shared key in multiple nodes, which threatens reliability if any of the nodes get compromised. A set is generated which consists of <key generated, number of occurrences it is used>. The sensors are chosen randomly and embedded with keys considering maximum limit before deployment. Using Eschenauer and Gligor's method shared key discovery and path key establishment is processed. To address the communication overhead to find a common key pseudo random function-based key pre-distribution scheme [30] was designed. The authority which embeds keys into the uses a hash function which determines which sensor can posses which key. Hence after deployment, the sensors using the hash function will be able to presume the common key in both the communication parties. If a common key is not found, path key establishment step is considered and the node goes along with this procedure.

Assuming that the adversary will not be able to eavesdrop on all the communication data exchanged between the sensor nodes, Tsai proposed a simple method to share keys [31] securely. In this technique each sensor node behaves as a beacon, where they broadcast string of random bits in their range of transmission. The receiving nodes within the transmission range collect some of the bits of the transmitted string. It then concatenates these random bits along with some hashing common bits and transmits the same. Hence a shared key is computed and used by two communicating parties.

Using a probabilistic key distribution scheme does not guarantee the availability of shared key between two communicating parties. If this scheme does not work out, path key establishment technique is considered. To enable this step, the nodes will have to shed some amount of energy. These devices are energy constrained, hence energy needs to be conserved. To adhere to this, BABEL key pre-distribution scheme [32] was designed. The model has adopted deployment of keys similar to [22] and has adopted path key establishment phase to discover shared keys. Merkle puzzle [33] is utilized, which employs to send a random set of strings compromising of <random string, key>. If the receiving node is able to decrypt this, the decrypted pair is considered as a shared key.

A post-deployment method was suggested by [34] to enhance connectivity of probability of key sharing schemes. This scheme integrates shared key concept and path key establishment concept similar to [22]. The node can request for a key from its neighbor, if it has a common key similar to the neighbor.

Localized encryption and authentication protocol (LEAP) [36] negotiate the shared key with their direct neighbors during secure bootstrapping time. Group key authentication scheme [37] has its base from [22]. Two-dimensional Gaussian distribution is assumed to design the protocol. The sensor nodes which are lying in the neighborhood are likely to have more number of common keys. Discovering shared keys and path key establishment stages follow the same instructions as in [22]. Attack probability-based key distribution scheme [38] has its foundation in [37]. The model tries to analyze and find solution for different probability attacks on a group.

Location-aware key establishment key distribution scheme [39], lays its foundation using Blundo method. The sensing region is logically divided into several sub-regions. A service sensor is chosen in a region using voting algorithm. The same constructs a bivariate t-degree symmetric polynomial along with two prime numbers. The two prime numbers generated has to satisfy Rabin's asymmetric cryptosystem. This is followed by broadcast of the public key by service node. Other nodes in the receiving end, generates a random number and dispatches the same along with its location coordinates. Service sensor node in turn generates univariate polynomial embedded within the coordinate information to the respective nodes. This information is encrypted using the respective random number received by the service sensor node from the other nodes of the network. To find the shared key, the two communicating parties interact with the same service sensor node.

Travel design based key distribution scheme [40] is being designed to overcome the disadvantages of group-based key distribution scheme. Combinatorial theory is used to build the model. The advantage of this scheme is it can be applied to field where different block overlap each other with predefined number of objects. This property of the model enhances security of inter-group and intra-group communication. Secure walking global positioning system [41] has explored the use of mobile robot, adopting a technique where the same performs node localization in addition to keying functionality. This technique serves full connectivity.

It is not possible to safeguard the data by using protection based algorithms, to enhance the security the intruders have to be detected and eliminated from the network. Doing this can provide the maximum security in the network. Some of the IDS based algorithms are summarized below-

In [11] the author has proposed a model for rule-based intrusion detection techniques. The study is divided into three phases. The foremost one is where the monitor nodes do the hearing and filter necessary data for analysis. In the second phase known as rule application phase, the counter is increased if any of the analysis fails. The data is compared with the pre-defined rule to evaluate the collected data. The third phase is intrusion detection phase where an alarm is raised if the number of failures is increased compared to the previous attempt.

[12] is being designed to identify possible malicious node based on received signal strength. Wormhole attack and HELLO attack is being tackled in this study. The energy of the received signal is compared with the energy of the signal observed around the network. 4 module schemes are being designed by the author in [13] to tackle sinkhole attack. The four modules include local packet monitoring module, local detection engine module, cooperative detection engine module and local response module. Fuzzy logic based intrusion detection is being modeled in [14]. Two concepts are being included in this model. First concept finds the ratio between proportions of reinforcement messages transmitted in the area to the number of sensing events in the area. The second is defined as number of hop counts between any two nodes in an area. Using these two concepts alarm is raised.

The author [15] has designed an IDS agent where the neighbors behave as intrusion detectors. In this model some neighbors are chosen to behave as IDS agents whose task is to optimally monitor its neighbor. The proposed model is distributive and cooperative kind. The study supports high density of nodes in the environment. An isolation table was suggested by the authors in [16] to detect the intrusions in energy effective way. Each level of node behaves as the detectors for the nodes at other level and notifies the base station of any malicious activity. Clustering based approach is considered in [17]. The cluster members monitor their respective cluster heads in time scheduled manner and vice versa. Cluster heads behaved as the detectors in [18] [19]. Cluster based hierarchical routing was considered in design. In [10] the author has considered local detectors modules. This module triggers any suspicion activity in its neighborhood. In [9] the author suggested an algorithm to tackle sinkhole attack. A list of suspicious nodes is being created using network flow graph. Multivariate technique/statistical-parametric technique based on chi-square test is implemented.

In [8] the authors have designed an algorithm which is real-time based. Arrival model for the traffic received by the sensor node was devised to detect any anomaly activity in the network. A sliding window multi level event was considered by which the algorithm maintained short term statistics of the traffic at different intervals of time. The author considered game theoretic environment [42] [43] where the attacker and detector belong to two different parties. Non cooperative and non-zero game model was considered to detect the anomalies in the environment under study.

The proposed model [45] provided solution to minimize communication overhead apart from detecting malicious node in the network. A distributed one-class quarter sphere support vector machines are utilized to detect the anomalies. The work is extended by mapping input space to higher dimensional space. A light weight method [46] was suggested by the author to detect the anomalies. The system information like neighbor list, routing tables, sleep/wake schedules, receive signal strength indication and MAC layer transmission schedules were considered while designing this algorithm. Multi-layer detectors in different layers of OSI stack were suggested. This protocol was mainly designed for outside attacks. An IDS based on packet level receive power anomalies was designed in [47]. The algorithm considered transceiver behaviors and packet arrival rates of neighboring nodes to detect the compromised node in the neighborhood.

In [48] the author considered packet marking and heuristic ranking algorithms were considered to identify bad nodes in the network. The packets are encrypted and padded before being transmitted. The packet mark suffixed to the data a packet which provides the origin information of the data to the base station. By utilizing this dropping ratio can also be calculated by the base station. The author [49] designed hierarchical trust management system to detect the inside attacker in the network under study. Stochastic Petri nets technique was employed to develop a probability model. The model is being utilized to analyze the protocol performance and validate subjective trust against objective trust based on ground truth node status.

IV. ASSUMPTIONS

The work is mainly designed to assess the level of security in the network against Sinkhole and Wormhole attacks. Various prevention and detection algorithms have been proposed by various authors. The paper considers the overall contributions and is designed to provide better and stronger security in the network.

The following assumptions are made in the work-

- The network is composed of nodes which are assigned a job to monitor the environment, process it, encrypt using a key and transmit to the base station.
- Some nodes in the network are being assigned as detector, which is assigned a job to monitor the activity of other nodes of the network. In this paper, a node inside the cluster and cluster head is given the task to monitor the nodes and send a report to the base station.
- Two types of attacks are being considered- Wormhole attack and Sinkhole attack.
- Wormhole attack is where the transmitted data is tunneled to a different location by the compromised nodes and replayed. This provides wrong information to the base station. To counteract to this kind of attack, a location based key can be utilized. Other technique is achieved by attaching a MAC key to the transmitted message or implementing time slots. This technique helps the nodes which fall in path (which is used to forward the packets) recognize the neighbor, if the data is not reliable data can be rejected (which helps to consume unwanted wastage of energy).
- Sinkhole attack is where the malicious node tries to divert the traffic towards itself. The node unknowingly transmits all the data to the compromised nodes. The malicious node can either modify the data before retransmitting the data to the sink or deny sending the data. To neutralize this kind of attack, detectors can be utilized to monitor the nodes in the network. One detector is present inside the cluster, which maintains the details of all the activity of the cluster members. Neighboring cluster head also behaves as detector which keeps the details of the detectors of the neighboring clusters.

V. SYSTEM PARAMETERS

Let S_{net} be the secured network (which does not have any compromised node in the network). To make the network secure against wormhole and Sinkhole attacks the following formulation and parameters are considered.

TABLE III
TABLE MAINTAINED BY DETECTOR OF THE CLUSTER

Node id	Cluster head id	Time	Number of bits transmitted	Time cluster head forwarded packets	No of bits transmitted
N_i	CH_i	T_i	T_{p1}	T_m	T_{pm}
N_j	CH_j	T_j	T_{p2}	T_n	T_{pn}

A. *Role of the detector*

The detector inside the cluster keeps a list of packets the nodes have dispatched in every session, time the packet was dispatched to the cluster head, the length of the message, time the cluster head forwarded the message, total length of the message forwarded by the cluster head. These details are represented in table 2.

In the table 3, two detectors of the clusters are under enquiry (report sent to the detector from the base station). The detectors in the clusters are evaluated. The detector D_i in the cluster C_i is under a control of smart intruder, which sends a false report at certain interval of time (not to get caught). But on continuous observation the summation report from multiple detectors in the neighbouring cells entraps the compromised detector.

TABLE IIIII
TABLE MAINTAINED BY NEIGHBORING CLUSTER HEAD

Cluster head	Time the data is transmitted	Detector under enquiry	Report is affirmative or not
CH_i	T_i T_j T_k T_l	D_i	True false true false
CH_j	T_j T_j T_k T_l	D_j	False False False False
CH_k	T_i	-	-

In the table the entries of the cluster C_j which is owns the detector D_j, generates only the false alarm. The report can be generated soon and the detector can be concluded as compromised node.

The work is designed such that the report is obtained from multiple sources and thus makes the network protected from false alarm.

B. Generating Linear programming formula

The main focus of the paper is to maximize security of the nodes and parallel utilizing reasonable amount of energy. Let N_{total} be the total number of nodes deployed in the network. The objective of the model is-

$$\textbf{Maximize } S_{net} \quad \text{------------------ (1)}$$

Let the buffer size of all the node set to B_{full}. Let T_P be the number of packets transmitted at any instant of time T_i. Let C_i be the number of cluster members of the clusters. Let CH_i be the cluster head. Let T_{delay} be the time limit to transmit the packets to the cluster head. Let $T_{transmit}$ be the transmission slot allotted by the cluster head CH_i to the cluster member C_i. Then the LP model would be-

$$T_p \leq B_{full} \quad \text{-------------- (2)}$$

$$|T_{transmit} - T_i| \leq T_{delay} \quad \text{----------- (3)}$$

$$T_p * C_i \leq \begin{cases} B_{full} * (C_i + CH_i) & \textit{Location based keys} \\ B_{full} * (C_i + CH_i + CH_{mac}) & \textit{Location independent keys} \end{cases} \quad \text{------------(4)}$$

$$T_p * C_i \geq TH_i \quad \text{------(5)}$$

The cluster head cross verifies the number of packets which are being dispatched by each cluster member. This number should not be greater than the buffer size. Equation (2) represents the above concept. From equation (3), portrays the transmission time of data packets from cluster member to its cluster head within the time delay. The cluster head aggregates all the packets of its cluster members, removes the redundant ones, attaches its own packet and forwards it to the next hop. The forwarded packet is being evaluated for its validity by the next hop CH_j. equation (4) is formulated for location based keys and location independent keys. equation (5) sets the threshold on number of packets which is to be transmitted from one hop to another (depends on the system configuration and user-defined threshold).

c. Simulated results

The simulation is done in c#. The parameters used in the simulation in listed in table 4. Tinynode 584 is deployed in the network. Considering the attack rate to be low, average and high the graph is being plotted.

TABLE IVV
PARAMETERS USED IN SIMULATION

Description	Parameters
Dimension of area	200m * 200m
Distribution	Uniform
Number of nodes in the cluster	6
Total number of nodes in network	240
Tinynode 584 configuration	
Data frame size	272 bits
Acknowledgment frame size	64 bits
Data bit rate	76 kbps
Preamble	6 bytes

i. Sinkhole attack

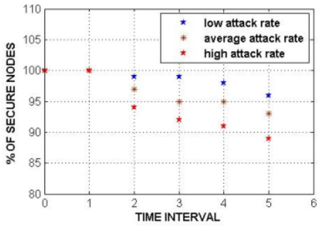

Fig 1 – illustration of sinkhole attack

This is one of the attacks [50-52] encountered when the data is transmitted from one end to another. The nodes under this attack publicize itself as a node closer to the base station. Other nodes unknowingly choose this compromised node to forward the data. By doing this the compromised node can replay the forwarded data and devastate the energy of other nodes in the path followed by them to reach the base station. Fig 1, depicts the result of sinkhole attack.

ii. Wormhole attack

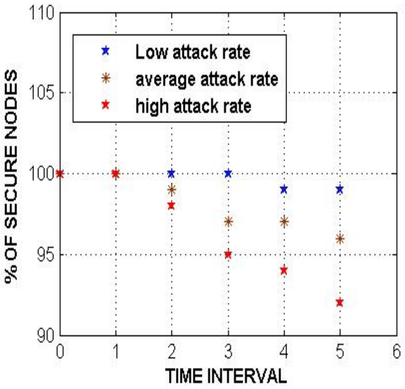

Fig 2 – illustration of wormhole attack

Wormhole attack [53-54] is a kind of attack where the intruder embezzles the packet from reaching the next hop (reliable one) ducts the packet to different location and retransmits it to the base station/next hop. Performing this activity provides a false illusion of the environment to the base station (about the environment). The base station may not be able to take accurate decision on time. The proposed model either utilizes location-based keys or attaches MAC key to minimize wormhole attack. Fig 2, portrays the wormhole attack.

VI. CONCLUSION

Wireless network is apt to different kinds of attacks compared to wired medium. Hence providing a security framework is essential where the data which is transmitted, source which transmits the data and destination which receives the data remains secure. In the work, linear programming model is constructed considering several constraints and objective function is formulated.

REFERENCES

[1] G.J. Pottie , W.J. Kaiser (2000) Wireless Integrated Network Sensors. Comm. ACM, vol. 43, issue 5, pp. 51-58.

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

[3] G. Simon, M. Maroti, A. Ledeczi, G. Balogh, B. Kusy, A. Nadas, G. Pap, J. Sallai, K. Frampton, Sensor network-based countersniper system, in: Proceedings of the Second International Conference on Embedded Networked Sensor Systems (Sensys), Baltimore, MD, 2004.

[4] J. Yick, B. Mukherjee, D. Ghosal, Analysis of a Prediction-based Mobility Adaptive Tracking Algorithm, in: Proceedings of the IEEE Second International Conference on Broadband Networks (BROADNETS), Boston, 2005.

[5] M. Castillo-Effen, D.H. Quintela, R. Jordan, W. Westhoff, W. Moreno, Wireless sensor networks for flash-flood alerting, in: Proceedings of the Fifth IEEE International Caracas Conference on Devices, Circuits, and Systems, Dominican Republic, 2004.

[6] T. Gao, D. Greenspan, M. Welsh, R.R. Juang, A. Alm, Vital signs monitoring and patient tracking over a wireless network, in: Proceedings of the 27th IEEE EMBS Annual International Conference, 2005.

[7] K. Lorincz, D. Malan, T.R.F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, S. Moulton, Sensor networks for emergency response: challenges and opportunities, Pervasive Computing for First Response (Special Issue), IEEE Pervasive Computing, October–December 2004.

[8] S.S. Doumit and D.P. Agrawal, "Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks", *in Proc. IEEE Military Communications Conference (MILCOM'03)*, 2003.

[9] E. Ngai, J. Liu and M. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks," *ICC'06*, Istanbul, Turkey, June 2006.

[10] I. Krontiris, Z. Benenson, T. Giannetsos, F. Freiling and T. Dimitriou, "Cooperative intrusion detection in wireless sensor networks", *Springer J. Wireless Sensor Networks*, pp. 263-278, 2009.

[11] Silva, A.P.R.D., M.H.T. Martins, B.P.S. Rocha, A.A.F. Loureiro and L.B. Ruiz *et al*., 2005. Decentralized intrusion detection in wireless sensor networks. Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks, (QSSWMN; 25),pp: 16-23. DOI: 10.1145/1089761.1089765

[12] Pires, W.R., T.H. De Paula Figueiredo, H.C. Wong and A.A.F. Loureiro, 2004. Malicious node detection in wireless sensor networks. Proceedings. 18th International, Parallel and Distributed Processing Symposium, (PDS' 04), pp: 1-7.

[13] I. Krontiris, T. Dimitriou and F.C. Freiling, "Towards Intrusion Detection in Wireless Sensor Networks", *Proc. 13th European Wireless Conference*, 2007.

[14] Chi, S.H. and T.H. Cho, 2006. Fuzzy Logic Anomaly Detection Scheme for Directed Diffusion Based Sensor Networks. Proceedings of the 3rd International Conference on Fuzzy Systems and Knowledge Discovery, (FSKD' 26), Springer-Verlag Berlin, Heidelberg, pp: 725-734. DOI: 10.1007/11881599_88

[15] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," *in Proc. IEEE Consumer Communications and Networking Conference*, 2006.

[16] R.C. Chen, C.F. Hsieh, Y.F. Huang, "A New Method for Intrusion Detection on Hierarchical Wireless Sensor Networks", *in Proc. ACM ICUIMC-09*, 2009.

[17] C.C. Su, K.M. Chang, Y.H. Kuo and M.F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks", *in Proc. IEEE Wireless Communications and Networking Conference*, 2005.

[18] A.A. Strikos, "A full approach for intrusion detection in wireless sensor networks", *School of Information and Communication Technology*, 2007.

[19] S. Rajasegarar, C. Leckie, M. Palaniswami, J.C. Bezdek, "Distributed Anomaly Detection in Wireless Sensor Networks", *10th IEEE Singapore International Conference on Communication systems*, 2006.

[20] Blom R, " An optimal class of symmetric key generation systems", In Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 1984.

[21]. Blundo C, Santis AD, Herzberg A, Kutten S, Vaccaro U, Yung M, "Perfectly secure key distribution for dynamic conferences", In Proceedings of the 29th International Cryptology Conference (CRYPTO), 1993.

[22] Eschenauer L, Gligor V, "A key management scheme for distributed sensor networks", In Proceedings of the Annual ACM Computer and Communications Security (CCS), 2002.

[23] Chan H, Perrig A, Song D. "Random key pre-distribution schemes for sensor networks.", In Proceedings of IEEE Symposium on Security and Privacy (S&P), 2003.

[24] Du W, Deng J, Han YS, Varshney P, "A pair-wise key pre-distribution scheme for wireless sensor networks", In Proceedings of the Annual ACM Computer and Communications Security (CCS), 2003.

[25] Çamtepe SA, Yener B. , "Combinatorial design of key distribution mechanisms for wireless sensor networks.", IEEE/ACM Transaction on Networking 2007; 15(2): 346–358.

[26] Lee J, Stinson DR. On the construction of practical key pre-distribution schemes for distributed sensor networks using combinatorial designs. ACM Transactions on Information and System Security (TISSEC) 2008; 11(2): 5:1–5:35.

[27] Çamtepe SA, Yener B, Yung M. , "Expander graph based key distribution mechanisms in wireless sensor networks.", In Proceedings of IEEE International Conference on Communications (ICC), 2006.

[28] Chan H, Perrig A. , "PIKE: peer intermediaries for key establishment in sensor networks. ", In Proceedings of the 24th IEEE Conference on Computer Communications (INFOCOM), 2005.

[29] Tague P, Poovendran R. ,"A canonical seed assignment model for key predistribution in wireless sensor networks.", ACM Transactions on Sensor Networks 2007; 3(4): Article 19.

[30] Pietro RD, Mancini LV, Mei A. , "Efficient and resilient key discovery based on pseudo random key pre-deployment", In Proceedings of International Parallel and Distributed Processing Symposium (IPDPS) — Workshop 12, 2004.

[31] Tsai S.C, Tzeng W.G, Zhou K.Y., "Key establishment schemes against storage bounded adversaries in wireless sensor networks.", IEEE Transactions on Wireless Communications 2009; 8(3): 1218–1222.

[32] Deng J, Han Y S ," Babel: using a common bridge node to deliver multiple keys in wireless sensor networks. ", In Proceedings of IEEE Global Telecommunications Conference (GLOBECOM), 2007.

[33] Merkle RC. Secure communications over insecure channels. Communication of ACM 1978; 21(4): 294–299.

[34] Law CF, Hung KS, Kwok YK. ,"A novel key redistribution scheme for wireless sensor networks. ", in Proceedings of the IEEE International Conference on Communications (ICC), 2007.

[35] I. Akyildiz, W. SU, Y. Sankarasubramaniam, E. Cayirci (2002) A Survey on Sensor Networks. IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114.

[36] Zhu S, Setia S, Jajodia S, " LEAP: efficient security mechanisms for large scale distributed sensor networks", in Proceedings of the Annual ACM Computer and Communications Security (CCS), 2003.

[37] Du W, Deng J, Han YS, Chen S, Varshney PK. A key management scheme for wireless sensor networks using deployment knowledge. In Proceedings of the 24th IEEE Conference on Computer Communications (INFOCOM), 2004.

[38] Chan S, Poovendran R, Sun M. A key management scheme in distributed sensor networks using attack probabilities. IEEE Global Communications Conference, Exhibition & Industry Forum (Globecom), 2005.

[39] Liu F, Cheng X. LKE: a self configuring scheme for location-aware key establishment in wireless sensor networks. IEEE Transactions on Wireless Communications 2008; 7(1): 224–232.

[40] Martin KM, Paterson MB, Stinson DR. Key predistribution for homogeneous wireless sensor networks with group deployment of nodes. ACM Transactions on Sensor Networks (TOSN) 2010; 7(2): Article 11.

[41] Mi Q, Stankovic JA, Stoleru R. Secure walking GPS: a secure localization and key distribution scheme for wireless sensor networks. ACM Conference on Wireless Network Security (WiSec), 2010.

[42] A. Agah, S.K. Das, K. Basu and M. Asadi, "Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach," *Proc. 3rdIEEE International Symposium on Network Computing and Applications(NCA'04)*, pp. 343-346, 2004.

[43] A. Agah and S.K. Das, "Preventing DoS attacks in wireless sensor networks: A repeated game theory approach", International Journal of Network Security, volume 5, number 2, pages 145-153, 2007.

[44] S. Rajasegarar, C. Leckie and M. Palaniswami, "Anomaly Detection in Wireless Sensor Networks", *IEEE Trans. Wireless Commun.*, 2008.

[45] S. Rajasegarar, C. Leckie, M. Palaniswami and J.C. Bezdek, "Quarter Sphere Based Distributed Anomaly Detection in Wireless Sensor Networks", *IEEE ICC '07*, Glasgow, U.K., June 2007.

[46] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," *J. High Speed Networks*, vol. 15, no. 1, pp. 33-51, 2006.

[47] I. Onat and A. Miri, "An Intrusion Detection System for Wireless Sensor Networks", *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2005.

[48] C. Wang, T. Feng, J. Kim, G. Wang and W. Zhang, "Catching Packet Droppers and Modifiers in Wireless Sensor Networks", *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, num. 5, pp. 835–843, 2012.

[49] F. Bao, R. Chen, M.J. Chang and J.H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust based routing and intrusion detection", *IEEE Trans. Network Service Management*, vol. 9, num. 2, pp. 169–183, 2012.

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

[51] Krontiris. I, Giannetsos. T, Dimitriou. T. (2008) Launching a Sinkhole Attack in Wireless Sensor Networks; The Intruder Side. IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, pg : 526-531, doi > 10.1109/WiMob.2008.83

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

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

[54] Honglong Chen, Wei Lou, Xice Sun, Zhi Wang (2010) 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, doi>10.1155/2010/627039.