THE GANG INJECTION FILTERING ALGORITHM BASED AUTHENTICATION SCHEME WITH SPATIAL CORRELATION METHOD FOR WIRELESS SENSOR NETWORKS

P. T. Kalaivaani[1] and A. Rajeswari[2]
[1]Department of Electronics and Communication Engineering, MNM Jain Engineering College, Chennai, India
[2]Department of Electronics and Communication Engineering, Coimbatore Institute of Technology, Coimbatore, India
E-Mail: ptkalaivaani@gmail.com

ABSTRACT

Wireless Sensor Network (WSNs) is a promising technology which supports large number of upcoming applications. Wireless Sensor nodes are deployed in unreceptive environment. In this environment ,sensor nodes are subjected to various attacks such as false data injection, eavesdropping, selective forwarding etc., The proposed work deals with security aspect in WSNs. Injected false data at sink level is a threat to WSNs security system. When the false data is injected at sink it creates a problem when updating the information at Base Station (BS) and also to filter the false data. False data injection leads to energy wastage in WSNs architecture. To minimize the energy wastage and to achieve better energy efficiency, to reduce the false data injection at sink node a novel method is proposed which drops the packets at node level and also in the sink level with Gang Injection Filtering Algorithm based Key Management Scheme. Spatial correlation concept is also adapted in the proposed work. Gang attack is considered in the proposed work and the parameters such as End to end delay, Throughput, Packet delivery ratio, Energy Consumption, Enrouted probability are analyzed using network simulator (NS2) tool.

Keywords: energy efficiency, false data injection, gang injection filtering algorithm, gang attack, wireless sensor networks (WSNs).

1. INTRODUCTION

A challenger can easily inject false data into WSNs field. Through the adversary can inject false data reports into the WSNs through cooperative nodes. Due to false data injection, base station will make a false decision. False decision depletes the energy of en-route nodes and the base station. It will act as a threat to WSNs life span. To detect and drop false data, number of en-route filtering schemes have been developed. Bandwidth Efficient Cooperative Authentication scheme for injected false data (BECAN) is an efficient method for filtering false data. Here, implements the BECAN scheme by using gang injection filtering algorithm with the help of NS2 simulation tool to increases the security & energy efficiency by adding Spatial correlation method.

A novel bandwidth efficient cooperative authentication scheme (BECAN) for filtering injected false data in a randomly deployed sensor nodes is discussed to save energy by early detecting and filtering majority of false data [1]. BECAN scheme is proposed with Co-operative bit compressed technique. Cluster based public infrastructure based on authentication of BS and security is proposed [2]. To ensure the confidentiality and integrity keys are established [2]. Spatial correlation based collaborative based medium access control technique is developed for transmission regulation of sensor nodes under a distortion constraint [3]. Event MAC and Network MAC filter the correlated data in wireless sensor network [3]. To capture and exploit correlation in wireless sensor networks several key elements are discussed [4]. For the development of efficient communication protocol it is necessary to set up a spatio-temporal correlation [4]. Study of security based mechanism for WSNs is proposed to highlight the vulnerabilities [5]. Different types of attacks are discussed [5]. For false report filtering two different types of fault localized schemes are proposed [6]. An effective secure routing for false data injection attack is proposed [7]. It resolves the contradiction between security requirement and additional load requirement to get required security [7]. Statistical en-route filtering mechanism is proposed to detect and drop false report during forward process [8]. Interleaved hop by hop authentication scheme is proposed [9]. The base station detects injected false data packets when no compromised nodes are identified [9]. Novel location based approach is proposed where the secret keys are bound in geographic locations [10].Hybrid authentication scheme is proposed [11].In field attack proof is introduced [12]. Novel key pre-distribution scheme is proposed. The scheme significantly develops the flexibility of the network [13]. Novel BECAN scheme to filter the injected false data with Cooperative bit compressed authentication scheme is proposed [14].

2. PROPOSED METHOD

The Proposed work formulates the WSNs with many sensor nodes. Nodes which are dark circled are considered as representative nodes in Fig.1. WSNs field is divided into many regions. Each region contains one representative node. The main task performed by each representative node is to collect the information from the other nodes in its corresponding region and forward the collected information to sink node (Base Station).Spatial correlation concept is adapted here. Spatial Correlation between the sensor nodes helps to prevent redundant data during transmission. In WSNs, when an event occurs in a sensor field, the nodes which are very nearer to that event area detect the event information and it is sensed by the neighborhood nodes. Every node transmits its own data to sink which is highly correlated that results in redundant transmission. The spatial correlation region is defined as the region in which all the sensor nodes send the readings which are similar in nature and therefore it is enough to send a single report to represent the correlation region [3].

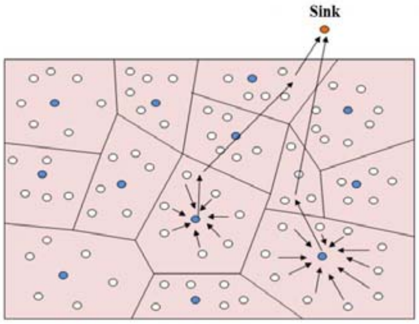

Figure-1. Representation of correlation region in WSNs.

The following steps are necessary to perform spatial correlation based energy efficient analysis

Step-1: Identify the event occurred in Sensor Field

Step-2: Fix the Source node (representative node from each region) and Target node (Sink)

Step-3: Find the Spatial correlation radius of the spatial correlated region

Step- 4: Split the correlation region into various parts

Step-5: Calculate the number of nodes involved in the sensing process in correlation region

Step-6: Representative nodes in the spatial correlation region collect the information from other nodes

Step-7: Identify & fix the total number of representative nodes in separated correlation region

Step- 8: Identify the routing method suitable to transmit the data from the source to destination.

Step-9: Forward the collected data from representative nodes to Base station (BS) Measure the energy consumption level of each region with respect to each node

Step-10: Repeat the same procedure when the next event occurs

Spatial correlation radius is represented by r_{corr}. It is the radius of correlation region. Correlation neighbor is defined as a node n_j is said to be the correlation neighbor of node n_i if the distance $d_{i,j}$ of the node n_i is smaller than r_{corr}.

$$corr\{S_i, S_j\} = \rho_{i,j} = K_v(d_{i,j}) = E\left[\frac{S_i, S_j}{\sigma^2{}_S}\right] \qquad (1)$$

(1) gives the correlation between the two nodes n_i and n_j located at the coordinates S_i, S_j. where $d_{i,j} = \rho_{si} - \rho_{sj}$. Where ρ denotes the distance between nodes n_i and n_j respectively, and $k_V(\cdot)$ is the correlation model or covariance model. The covariance function is assumed to be non-negative and decreases monotonically with the distance [3].

a) GANG ATTACK WITH INJECTION OF FALSE DATA

The proposed network model deals with gang attack for injecting false data at sink node. When the false data is injected at node level, it modifies and collapses the actual functionality of individual sensor nodes. When false data is injected at sink level, it disturbs the actual information available in sink node. The information available at sink nodes is collected from many different representative nodes from different correlation region. It is necessary to perform filtering operation on the injected false data. Filtering is possible at node level and sink level. The proposed scheme is sink level based filtering mechanism. In the existing methods, denial of service attack and Sybil attack [1], [5] were proposed. This study considers gang attack scheme. Gang attack is occurred due to group of sensor nodes around the source node. Due to the aggregation of nodes which are nearer to source node the false data is injected at high level at source node then the source node becomes ready to transfer the injected false data details to sink node. To identify the gang attack and to prevent the gang attack it is necessary to identify the position of each sensor node involved in the sensing field. Using vector quantization algorithm [3], the code book is updated. Code book contains all the position details of sensors involved in the sensing process.

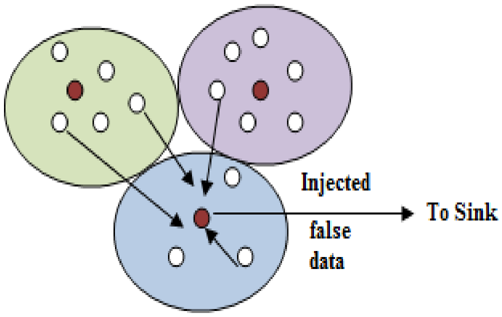

Figure-2. Gang attack.

Figure-2 shows the gang attack scheme. Source nodes are represented by red circles. Neighborhood nodes are represented as normal circles. Each node position is updated in the codebook of vector quantization method. Similar way the nodes which are communicated with neighborhood region’s source node along with position also updated in codebook.

b) Gang injection filtering algorithm

The Gang Injection filtering algorithm is based on polynomial arithmetic, in particular, on computing the remainder of dividing one polynomial in GF(2) (Galois field with two elements) by another. It is a little like treating the message as a very large binary number, and computing the remainder on dividing it by a fairly large prime such as $2^{32} – 5$. Intuitively, one would expect this to give a reliable checksum.

A Polynomial in GF(2) is a polynomial in a single variable *x* whose coefficients are 0 or 1. Addition and subtraction are done modulo 2—that is, they are both the same as the *exclusive or* operator. For example, the sum of the Polynomials $x^3 + x + 1$ and $x^4 + x^3 + x^2 + x$ is $x^4 + x^2 + 1$, as is their difference. These polynomials are not usually written with minus signs, but they could be, because a coefficient of –1 is equivalent to a coefficient of 1.

Multiplication of such Polynomials is straightforward. The product of one coefficient by another is the same as their combination by the logical *and* operator, and the partial products are summed using *exclusive or*. Multiplication is not needed to compute the gang injection filtering algorithm checksum. Division of Polynomials over GF (2) can be done in much the same way as long division of Polynomials over the integers. Below is an example. The reader might like to verify that the quotient of $x^4 + x^3 + 1$ multiplied by the divisor of $x^3 + x + 1$, plus the remainder of $x^2 + 1$, equals the dividend.

The gang injection filtering algorithm method treats the message as a polynomial in GF(2). For example, the message 11001001, where the order of transmission is from left to right (110…) is treated as a representation of the polynomial $x^7 + x^6 + x^3 + 1$. The sender and receiver agree on a certain fixed polynomial called the *generator* polynomial. For example, for a 16-bit gang injection filtering algorithm has chosen the polynomial $x^{16} + x^{12} + x^5 + 1$, which is now widely used for a 16-bit gang injection filtering algorithm checksum. To compute an *r*-bit gang injection filtering algorithm checksum, the generator polynomial must be of degree *r*. The sender appends *r* 0-bits to the *m*-bit message and divides the resulting polynomial of degree $m + r – 1$ by the generator polynomial. This produces a remainder polynomial of degree $r – 1$ (or less). The remainder polynomial has *r* coefficients, which are the checksum. The quotient polynomial is discarded. The data transmitted (the code vector) is the original *m*-bit message followed by the *r*-bit checksum.

There are two ways for the receiver to assess the correctness of the transmission. It can compute the checksum from the first *m* bits of the received data, and verify that it agrees with the last *r* received bits. Alternatively, and following usual practice, the receiver can divide all the $m + r$ received bits by the generator poly-nomial and check that the *r*-bit remainder is 0. To see that the remainder must be 0, let *M* be the polynomial representation of the message, and let *R* be the polynomial representation of the remainder that was computed by the sender. Then the transmitted data corresponds to the polynomial $Mx^r – R$ (or, equivalently, $Mx^r + R$). By the way *R* was computed, we know that $Mx^r = QG + R$, where *G* is the generator polynomial and *Q* is the quotient (that was discarded). Therefore the transmitted data, $Mx^r – R$, is equal to *QG*, which is clearly a multiple of *G*. If the receiver is built as nearly as possible just like the sender, the receiver will append *r* 0-bits to the received data as it computes the remainder *R*. But the received data with 0-bits appended is still a multiple of G, so the computed remainder is still 0.

That is the basic idea, but in reality the process is altered slightly to correct for such deficiencies as the fact that the method as described is insensitive to the number of leading and trailing 0-bits in the data transmitted. In particular, if a failure occurred that caused the received data, including the checksum, to be all-0, it would be accepted. Two simple observations: For an *r*-bit checksum, *G* should be of degree *r*, because otherwise the first bit of the checksum would always be 0, which wastes a bit of the checksum. Similarly, the last coefficient should be 1 (that is, *G* should not be divisible by *x*) because otherwise the last bit of the checksum would always be 0 (because $Mx^r = QG + R$, if *G* is divisible by *x*, then *R* must be also). The following facts about generator polynomials are proved.

- If *G* contains two or more terms, all single-bit errors are detected.

- If *G* is not divisible by *x* (that is, if the last term is 1), and *e* is the least positive integer such that *G* evenly divides $x^e + 1$, then all double errors that are within a frame of *e* bits are detected. A particularly good Polynomial in this respect is $x^{15} + x^{14} + 1$, for which $e = 32767$.
- If $x + 1$ is a factor of *G*, all errors consisting of an odd number of bits are detected.

- An *r*-bit gang injection filtering algorithm checksum detects all burst errors of length $\le r$. (A burst error of length *r* is a string of *r* bits in which the first and last are in error, and the intermediate $r – 2$ bits may or may not be in error.)

The generator polynomial $x + 1$ creates a checksum of length 1, which applies even parity to the message. (Proof hint: For arbitrary $k \ge 0$, what is the remainder of dividing x^k by $x + 1$)It is interesting to note that if a code of any type can detect all double-bit and single-bit errors, then it can in principle correct single-bit errors. To see this, suppose data containing a single-bit error is received. Imagine complementing all the bits, one at a time. In all cases but one, these results in a double-bit error, which is detected. But when the erroneous bit is complemented, the data is error-free, which is recognized. In spite of this, the gang injection filtering algorithm method does not seem to be used for single-bit error correction. Instead, the sender is requested to repeat the whole transmission if any error is detected.

For Spatial Correlation Based Energy Efficient Analysis,
The requirements are,

- Sensor node deployment
- En-routing technique
- Sink verification

- Key management scheme

c) Sensor node deployment

Assume Uniform distribution of sensor nodes over the given sensor field. Set of sensor nodes are assumed as x_1,x_2,x_3…. available in (6)

$$X = \{x_1, x_2, x_3, x_4.....\} \qquad (2)$$

The uniformly distributed Sensor nodes are co-operatively establish or adjust their routing to the sink by using dijkstra shortest path algorithm. Once an event occurs the report can be immediately relayed over the already established routing path.

d) En-Routing filtering

When each sensor node has sensed the data and sent to the sink via the routing path and It checks the integrity of the message and the timestamp T. The data integrity verification will be done in en-route nodes, if the timestamp is out of date, the message will be discarded. If the sink receives the report successfully it also checks the integrity of the message and the timestamp. If the timestamp is out of date, the message will be immediately discarded. En routing Probability can be tested in the following way in proposed analysis.EFP is the enroute filtering probability.EPF is the ratio between number of false data filtered by enroute nodes to the total number of false data

e) Sink verification

The sink verifies the report received from source node. If the data with time stamp is out of date then the input message is immediately discarded from sink node. The sink also verifies the source side private keys before it accepts the report [1].

a) Key management scheme

For the security analysis, a pair of keys used to send the source information to destination information. 16 bit and 18 bit unsigned values are used as the keys to attach with actual information. Access is denied for unauthorized users. Therefore the input data stream is properly encoded along with key values to transfer to the far end [1].

3. RESULTS AND DISCUSSIONS

The network area of 1500x1500 is considered with 100 numbers of nodes with 2MHz bandwidth. Data rate is 250kbps with transmitting and receiving power level of 1mW. The parameters such as bandwidth, delay, energy consumption, using Gang Injection Filtering Algorithm based Authentication Scheme, The following Parameters are analyzed. The Parameters such as End to End Delay, Packet Delivery Ratio, Average Throughput, Energy Consumption for various rounds. End to End delay is analyzed for two different rounds for single attack and Gang Attack. Gang attack is Marked in red color and Single attack is marked in green color. When the rounds are increased in number Gang attack delay value is lowered compared with single attack.

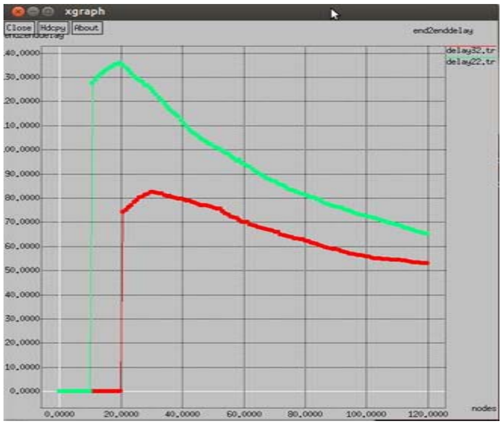

Figure-3. Nodes vs end to end delay.

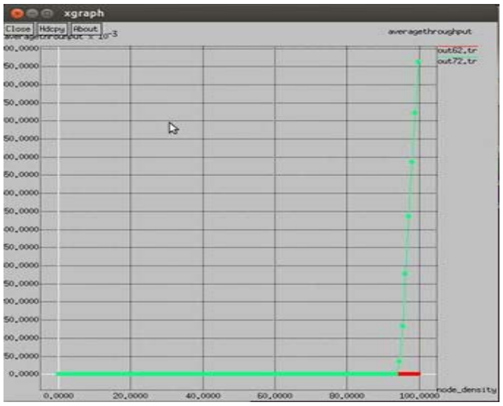

Figure-4. Node density vs average throughput.

Average Throughput of Single attack is very high compared with single attack for various rounds.

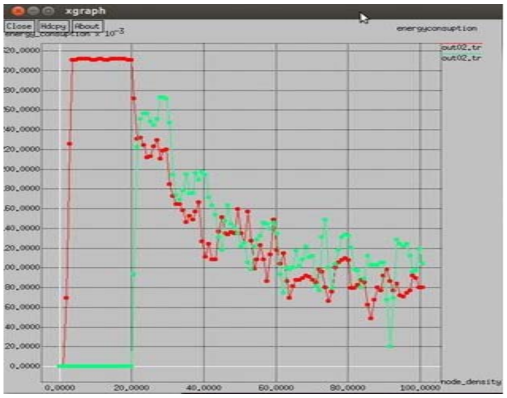

Figure-5. Node density vs energy consumption.

Energy consumption level of gang attack is very high than compared with single attack. Because during gang attack, the false data is injected at node level as well as in the sink level.

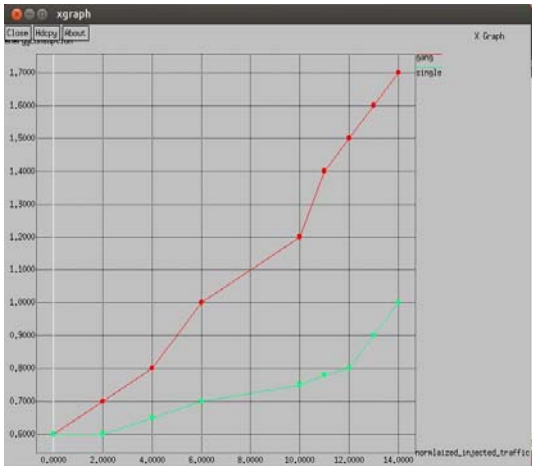

Figure-6. Normalized injected traffic vs energy consumption.

When the Packets are in the queue, The energy consumption analysis is carried out for single and gang attack. Gang attack shows higher energy consumption level than single attack.

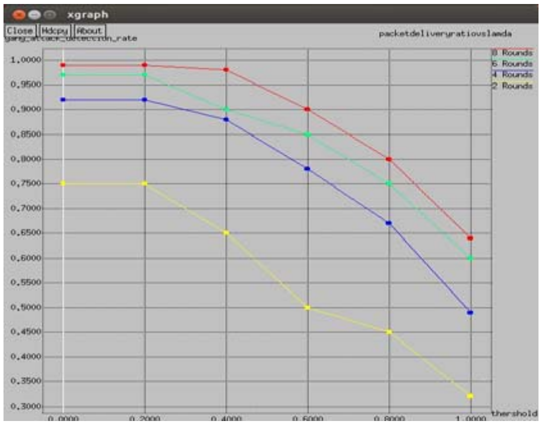

Figure-7. Threshold vs gang attack injection rate.

Gang attack injection rate is analyzed with respect to packet delivery ratio for various set of rounds. Initially the rounds are gradually increased from two to eight based on that the calculation is completed. For all the rounds, gang attack injection attains the maximum threshold except the initial round. In the Initial round, it randomly touches the Peak value.

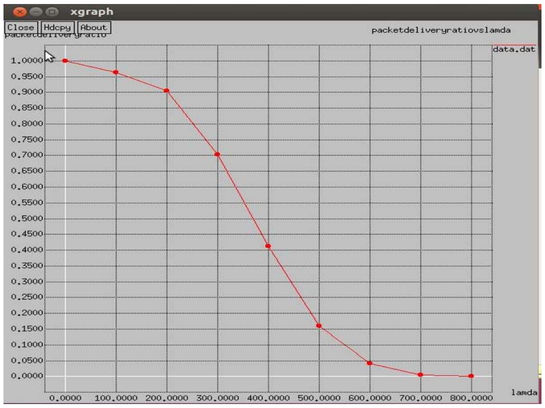

Figure-8. Lamda vs packet delivery ratio.

Packet delivery ratio is analyzed with respect to lamda. Lamda is known as packet inter arrival time .When Lamda value increases the value of packet delivery ratio is also good.

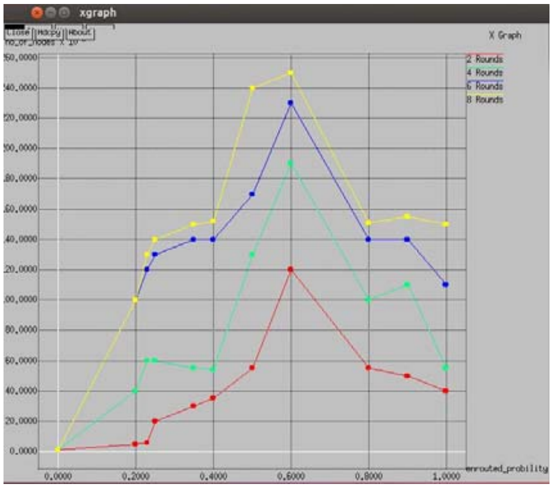

Figure-9. En routed probability vs number of nodes.

The above graph depicts the value of enrouted probability for various set of nodes. When Node value increases the values of enrouted probability also attains maximum value.

4. CONCLUSION AND FUTURE WORK

The Gang Injection Filtering Algorithm based Authentication Scheme with Spatial Correlation method provides better Energy Efficiency and Packet Delivery Ratio, Average Throughput, End to End delay with good Enroute Probability. Gang attack based energy efficiency scheme achieves reliability, high en-routing filtering probability. Due to its simplicity, it can be applied to fast and distributed authentication scheme. Proposed work concentrated on dropping of filtered packet at head node level and sink level. In future, it is possible to implement the work for node level with different security based algorithms. The proposed work concentrates for 100 number of nodes and the performance analysis is carried out. In future, Gang Injection filtering algorithm can be applied to multiple number of mobile compromised sensor nodes to analyze the Energy Efficiency performance of WSNs.

REFERENCES

[1] Rongxing Lu and Xiaodong Lin *et al.* 2012. “BECAN: A Bandwidth –Efficient Cooperative Authentication Scheme for Filtering injected False Data in Wireless Sensor Networks”, IEEE transactions on Parallel and Distributed Systems, Vol. 23. No. 1, Jan DOI:10.1109/TPDS.2011.95

[2] Benamar Kadri and Djilalli Moussaoui *et al.* 2012. “An Efficient Key Management Scheme for Hierarchical Wireless Sensor Networks”, Wireless Sensor Network, Vol. 4, pp. 155-161, DOI: 10.4236/wsn.2012.46022.

[3] Mehmet C., Vuran and Ian F. Akyildiz. 2006. “Spatial Correlation – Based Collaborative Medium Access Control in Wireless Sensor Networks” IEEE / ACM Transaction on Networking, Vol.14, No.2.

[4] Vuran M. C. *et al.* 2004. “Spatio-temporal correlation: theory and applications for wireless sensor networks. Comput. Networks Journal (Elsevier), Vol. 45, No. 3, pp.245-259.

[5] Martins D. and Guyennet H. 2010. “Wireless Sensor Networks Attacks and Security Mechanisms: A Short Survey”, Proc. of 13th International Conference on Network Based Information System”, pp.313-320,Sept. http://dx.doi.org/10.1109/NBiS.2010.11.

[6] L. Zhou and C. Ravishankar. 2005. “A Fault Localized Scheme for False report Filtering in Sensor Networks,” Proc of International Conference on Pervasive Services (ICP’05), pp.59-68, July.

[7] Z. Zhu, Q. Tan and P. Zhu. 2007. “An effiective secure Routing for False data injection Attack in Wireless Sensor Network”, Proc of 10th Asia-Pacific Network Operations and Management Symp. (APNOMS’07), pp.457-465.

[8] F. Ye, H. Luo, S. Lu and L. Zhang. 2004. ”Statistical En-route detection and filtering of injected false data in sensor network,” Proc. IEEE INFOCOM’04 , March.

[9] S. Zhu and S. Setia *et al.* 2004. “ An Interleaved Hop by Hop Authentication Scheme for filtering of Injected fasle data in Sensor Networks”,Proc.of IEEE Symposium on Security and privacy.

[10] H. Yang and F. YEY. Yuan *et al.* 2005. ”Toward Resilient Security in wireless Sensor Networks”,Proc of sixth ACM International Symposium on Mobile and Adhoc Networking and computing (Mobihoc’05), pp.34-45.

[11]Shahina K and Anand Pavithran. 2013. “Filtering Scheme for injected false data in WSN”,IOSR Journal of Computer Engineering,Vol.13, Issue 6, pp.29-31.

[12] Zheng Wang and Xiaodong Lee *et al.* 2008. “ In-Field Attack Proof of Injected False Data in Sensor Networks”, Journal Of Communications, Vol. 3, no. 6.

[13]T. Anbalagan and S. Madhavi. 2014. “Filtering False data in Wireless network using Cluster node and Key Management”, ISR National Journal of Advanced Research in Computer Science Engineering and Information Technology,Vol.1, ISs.1,May.

[14] D. Bharathidasan and S. Murugesan. 2013. “Key Management Scheme for Preventing False Data in Wireless Sensor Network”, International Journal of Electronics Communication and Computer Technology (IJECCT), Vol. 3, Issue 1, January.