Enhanced BECAN Based En-Route filtering schemes for injected false data in Wireless Sensor Networks

J.Ghayathri[#1], S.Poornima[*2]

#1Associate Professor, Department of Computer Science(PG) , Kongu Arts and Science College(Autonomous), Erode, India

**2 M.Phil. Research Scholar, Department of Computer Science(PG), Kongu Arts and Science College,(Autonomous),Erode, India*

Abstract: *Wireless device networking is an associate rising technology, which supports several rising applications as a result of their low price, tiny size and communication over short distances. False Data call depletes the energy of en-route nodes to the base station. We implements the BECAN (Bandwidth Efficient Co-operative Authentication) theme and will increase the protection by adding Hybrid Authentication Scheme (HAS). LEACH (Low Energy Adaptive Clustering Hierarchy) method is used to lower the energy consumption required to create and maintain clusters in order to improve the life time of a Wireless Sensor Network. The proposed system to impress the performance on energy consumption, data security and the communication cost.*

Keywords — *False data injection, Wireless Sensor Networks, Hill Climbing Method***.**

I. INTRODUCTION

A. Network

A Network is a group of two or more computer system linked together.[11]

A **client** is a computer program that, as part of its operation, relies on sending a request to another computer program (which may or may not be located on another computer). For example, web browsers are clients that connect to web servers and retrieve web pages for display.

A **server** is a computer program or a machine that waits for requests from other machines or software (clients) and responds to them. The purpose of a server is to share data or hardware and software resources among clients his document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website. In computing, a **sink** or **event sink** is a class or function designed to receive incoming events from another object or function.

In computer networking, **source routing**, also called **path addressing**, allows a sender of a packet to partially or completely specify the route the packet takes through the network. In contrast, in non-source routing protocols, routers in the network determine the path based on the packet's destination.

In communication networks, a **node** is a connection point, a redistribution point, or a communication endpoint (e.g. data terminal equipment).

In computer networking, the term **Gang aggregation** applies to various methods of combining (*aggregating*) multiple network connections in parallel in order to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links should fail. [12]

B. En-route Filtering Schemes

Five types of En-routes filtering schemes are available:

1. Statistical En-route filtering (SEF)
2. Commutative Cipher based En-route Filtering scheme (CEF)
3. Secure Ticket-Based En-route Filtering Scheme (STEF)
4. Dynamic En-route Filtering (DEF)
5. Band-width Efficient Co-operative Authentication scheme (BECAN)

Statistical en-route filtering is the first en-route filtering scheme (SEF) to address the fabricated report injection attacks in the presence of compromised nodes. [1] Commutative Cipher based En-route Filtering scheme (CCEF) drops fabricated reports en-route without symmetric key sharing. [4] In Secure Ticket-Based En-route Filtering Scheme (STEF), ticket concept is introduced to drops false messages en-route.[5] Dynamic En-route Filtering (DEF) is based on clustering. [6] Finally BECAN is band-width efficient co-operative authentication scheme for filtering injected false data. [7]

The three main contributions of Wireless Sensor Networks are:

1. The random graph characteristics of wireless sensor node deployment, and estimate the probability of k-neighbors, which provides the necessary condition for BECAN authentication; [13]

2. The BECAN scheme to filter the injected false data with cooperative bit-compressed authentication technique. With the proposed mechanism, injected false data can be early detected

and filtered by the en-route sensor nodes. In addition, the accompanied authentication information is bandwidth-efficient; [2]

3. A custom Java simulator to demonstrate the effectiveness of the proposed BECAN scheme in terms of en-routing filtering probability and false negative rate on true reports.

Sensor networks are collection of sensor nodes which co-operatively send sensed data to base station. Wireless Sensor Networks (WSN) offer an increasingly sensor nodes need less power for processing as compared to transmitting data.

C. False data injection

False data injection attack, first several sensor nodes are compromised by an attacker. When any sensor node is compromised then the attacker accessing all the key materials to stored in the compromised nodes, the nodes can be processed and send the false data to the sink. [16] Due to this false event is triggered and the false report sends to the sink.

The adversary may inject false measurement reports to be disrupting the small grid operation through the compromised meters and sensors. Those attacks denoted as false data injection attacks. It can disrupt the grid system state estimation. It can disrupt the energy distribution.

It could paralyze the entire network quickly. When network is compromised it is difficult to find a node because the symmetric key techniques are used in most of these filtering mechanisms. Filtering mechanism generates false data reports that the compromised node abuses its keys and degrade to the reliability of the filtering mechanisms.

.

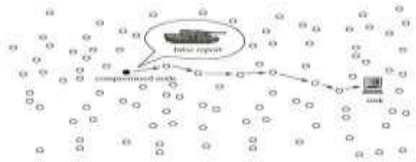


Fig.1. Wireless sensor network

II. *COMPARISON OF VARIOUS METHODS USED FOR WIRELESS SENSOR NETWORKS* LAYOUT

WSN is a Wireless Sensor Network that consists of base stations and number of nodes. These networks are used to monitor physical and environmental conditions like sound, pressure, temperature and co-operatively pass data through network to a main location. [9]

A Wireless Sensor Network is a group of specialized transducers with a communications infrastructure for monitoring and recording conditions at diverse locations commonly monitored parameters are temperature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant level, and vital body function.

A. Statistical En-route Filtering (SEF)

Statistical en-route filtering (SEF) is the first en-route filtering scheme to address the fabricated report injection attacks in the presence of compromised nodes and introduce an en-route filtering framework. [1]

B. Commutative Cipher based En-route Filtering (CCEF)

In Commutative Cipher Based En-route Filtering (CCEF), each node is preloaded with a distinct authentication key. [4]

C. Secure Ticket-based En-route Filtering (STEF)

Secure Ticket-Based En-route Filtering (STEF) uses a ticket concept, where tickets are issued by the sink and packets are only forwarded if they contain a valid ticket. [5]

D. Dynamic En-route Filtering (DEF)

In Dynamic En-route Filtering scheme (DEF) scheme, a legitimate report is endorsed by multiple sensing nodes using their own authentication keys. [6]

E.Bandwidth Efficient Co-operative Authentication (BECAN)

In Bandwidth Efficient Cooperative Authentication (BECAN) scheme, each node requires k number of neighbours for Co-operative Neighbour Router (CNR) based authentication. [2]

F. Projective clustering approach for the detection of outlier a non-axis-aligned subspaces

A non-axis-aligned subspace cluster S is a pair(R,W), where R _ {r1, r2, . . . , rm} is a subset of the rows and W is a collection of vectors {w1,w2, . . . ,wD}, where wi 2 Rp. [10].

III. *METHODOLOGY*

The framework for the proposed scheme for CBA authentication:

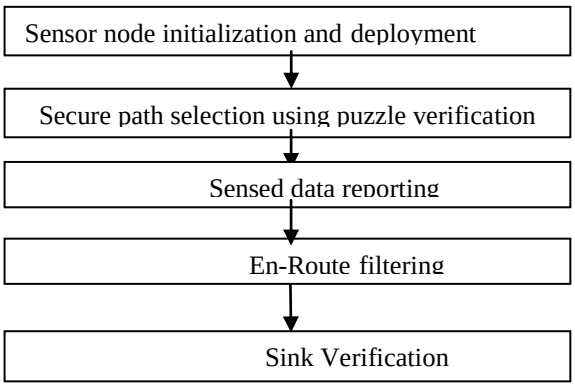


Fig.2. CBA Authentication

A. Description of BECAN authentication

The BECAN authentication scheme consists of two phases: sensor nodes initialization and deployment, and sensed results reporting protocol.

A Co-operative Bit-Compressed Authentication (CBA) scheme for filtering injected false data in Wireless Sensor Networks (WSN) [3]. The two main phases are:

A. Safe path selection.

B. Authentication and verification of sensed data.

a. Sensor Nodes Initialization and Deployment

Given the security parameter k, the sink first chooses an elliptic curve defined over, where p is a large prime and G is a base point of prime order q with. Then, the sink selects a secure cryptographic hash function, where. Finally, the sink sets the public parameters as prams. To initialize sensor nodes N= {n1, n2, n3…..} the sink invokes the sink deploys these initialized sensor nodes at a CIR in various ways, such as by air or by land. Without loss of generality, we assume that all sensor nodes are uniformly distributed in CIR after deployment.

b. Sensed Result Reporting Protocol

When a sensor node generates a report m after being triggered by a special event, e.g., a temperature change or in response to a query from the sink, it will send the report to the sink via an established routing.

The report m generated by sensor node by sensing of any parameters is send to the sink via, established shortest and safest path selected. [7]

c. En-Routing Filtering

When each sensor node Ri, ($1 \leq i \leq l$), along the routing RN0 receives (m, T, MAC) from its upstream node, it checks the integrity of the message m and the timestamp T. If the timestamp T is out of date, the message (m, T, MAC) will be discarded. If the returned value is "accept," Ri will forward the message (m, T, MAC) to its downstream node, Otherwise, (m, T, MAC) will be discarded.

d. Sink Verification

If the sink receives the report (m, T, MAC), it checks the integrity of the message m and the timestamp T. If the timestamp is out of date, the report (m, T, MAC) will be immediately discarded. Otherwise, the sink looks up all private keys kis of Ni, $0 \leq i \leq k$.

Sink on receiving the report checks the integrity of *R* and timestamp T. If T is outdated *R* is rejected otherwise *R* undergoes sink verification.

Sensor Node Initialization

The key server generates unique public and private keys for each sensor node and sink. These keys will be shared to the sensor nodes when they start.

CNR Based MAC Generation

CNR based Mac generation is used by the sensor nodes for generating authentication message. This technique uses Elliptic curve cryptography and DES algorithm.

CNR Based MAC Verification

The authentication message was sent by the sensor node using ECC algorithm verifies by the sink.

Sink Verification

The sink verifies each message sent by sensor nodes whether it is valid or invalid

B. Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems, such as the RSA algorithm, are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. Elliptic Curve Cryptography was used to send the data as encrypt and decrypt. [15]

C. Design Rationale

To filter the false data injected by compromised sensor nodes, the BECAN adopts cooperative neighbour router (CNR)-based filtering mechanism.

CNR-based mechanism, when a source node N0 is ready to send a report m to the sink via an established routing path RN0: [R1 -> R2 ->. . Rl-> Sink], it first resorts to its k neighbouring nodes NN0: {N1, N2, . . .,Nk} to cooperatively authenticate the report m, and then sends the report m and the authentication information MAC from N0 U NN0 to the sink via routing RN0. [46]

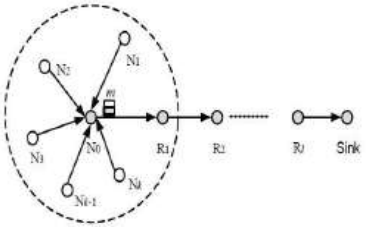


Fig.3 CNR based mechanism

D. Network Model

We consider a typical wireless sensor network which consists of a sink and a large number of sensor nodes N = {N0, N1, . . .} randomly deployed at a certain interest region (CIR) with the area S. Sink is liable for initializing the sensor nodes and collecting data by these sensor nodes and sink is considered to be powerful and trustable data collection device, since it has enough storage and computational capabilities. In a location each sensor node will be stationary. We assume that each sensor node has a unique nonzero identifier for differentiation purpose. In this case the communication will be bidirectional, i.e., two sensor nodes within their wireless transmission range (R) may communicate with each other. Therefore, if a sensor node is close to the sink, it can directly contact the sink.

F. Security Model

Since a wireless sensor network is unattended, a malicious adversary may readily launch some security attacks to degrade the network functionalities. In addition, due to the low-cost constraints, sensor nodes N ={N0,N1, . . .} are not provided with costly tamper-proof device and in an unprotected wireless sensor network it can easily compromised. [7] A can compromise a fraction of sensor nodes and obtain their stored keying materials. Then, after being controlled and reprogrammed by the adversary A, these compromised sensor nodes can collude to launch some injected false data attacks.

G. Sink Verification

If the sink receives the report (m, T, MAC), it checks the integrity of the message m and the timestamp T. If the timestamp is out of date, the report (m, T, MAC) will be immediately discarded. Otherwise, the sink looks up all private keys of Ni, 0 ≤ i ≤ k.

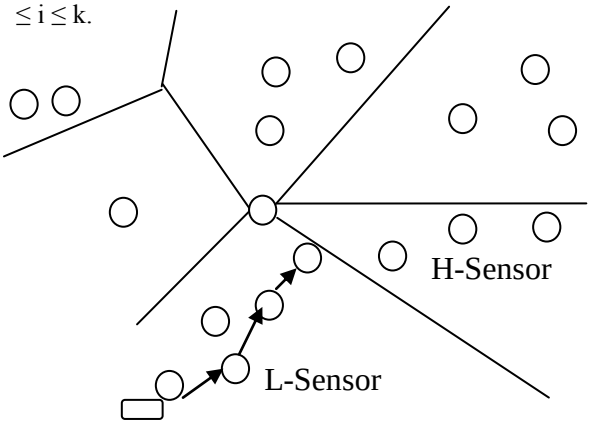


Fig.4 Sink Verification

H. Reliability of the BECAN scheme

In addition to the high (en-routing) filtering probability, the BECAN scheme also has high reliability, i.e., even though some sensor nodes are compromised, the true event reports still can reach the sink with high probability. [14]

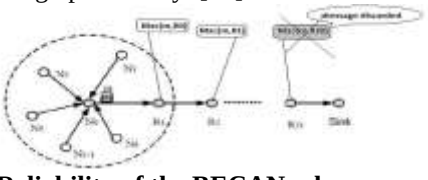


Fig.5 Reliability of the BECAN scheme

Let FNR be the false negative rate on the true reports and tested as

FNR=Number of true data that cannot reach the sink/Total number of true data

FNR=Number of true data that cannot reach the sink/Total number of true data

If FNR is small, the BECAN scheme is demonstrated high reliability. FNR can be increased by selectively dropping true report attack. Thus, for fairness, we only consider FNR that caused by 1) the number of uncompromised neighbouring sensor nodes being less than k, 2) Some compromised sensor nodes polluting the true report. It can be seen, when the number of independent reports increases, the FNR decreases. [8]

False Negative Rate (FNR)

FNR= Number of true data that cannot reach the sink/Total number of true data If FNR is small then the high reliability.

En-Route Filtering Probability (FPR)

FPR= Number of false data filtered at en-route nodes /Total number of false data

The en-route filtering probability FPR in terms of different number of en-routing nodes.

As the number of routing nodes increases, FPR increases.

Reaffliations per unit time

Reaffiliations per unit time imply the redundancy of transmitted data.

Throughput

Throughput= Number of packet received /Time

Energy consumption

The majority of the false data injection can be filtered by BECAN scheme within the short number of hops during the transmission

I. Hill Climbing Algorithm

```
currentNode = startNode;
  loop do
    L = NEIGHBORS(currentNode);
    nextEval = -INF;
    nextNode = NULL;
    for all x in L
      if (EVAL(x) > nextEval)
          nextNode = x;
          nextEval = EVAL(x);
    if nextEval <= EVAL(currentNode)
      //Return current node since no better neighbors
exist
       return currentNode;
    currentNode = nextNode;
  currentPoint = initialPoint;    // the zero-magnitude
vector is common
  stepSize = initialStepSizes;    // a vector of all 1's is
common
  acceleration = someAcceleration; // a value such as
1.2 is common
  candidate[0] = -acceleration;
  candidate[1] = -1 / acceleration;
  candidate[2] = 0;
  candidate[3] = 1 / acceleration;
  candidate[4] = acceleration;
  loop do
    before = EVAL(currentPoint);
    for each element i in currentPoint do
      best = -1;
      bestScore = -INF;
```

```
    for j from 0 to 4        // try each of 5 candidate
locations
        currentPoint[i] = currentPoint[i] + stepSize[i]
* candidate[j];
        temp = EVAL(currentPoint);
        currentPoint[i] = currentPoint[i] - stepSize[i]
* candidate[j];
        if(temp > bestScore)
            bestScore = temp;
            best = j;
      if candidate[best] is not 0
        currentPoint[i] = currentPoint[i] + stepSize[i]
* candidate[best];
        stepSize[i] = stepSize[i] * candidate[best]; //
accelerate
    if (EVAL(currentPoint) - before) < epsilon
      return currentPoint;
```

IV. EXPERIMENTAL RESULTS

A. MAC Implementation

Filtering the false injected data is the main problem in wireless sensor networks. The proposed scheme is used to filter the false data injection by verifying the MAC of every node.

In model sink, cluster head, and sensor node have been designed, sink receives message from sensor node, while establishing sensor node the system identifies the cluster head which is also one of the sensor node, sensor node always sends data via cluster head, then to sink.

When each Sensor Node receives message m, timestamp T and MAC, the Sensor Node checks the integrity of message m, timestamp T, if timestamp T is out of date, the received message m, timestamp T and MAC will be discarded.

Chart 1 AVERAGE DELAY PROBABILITIES

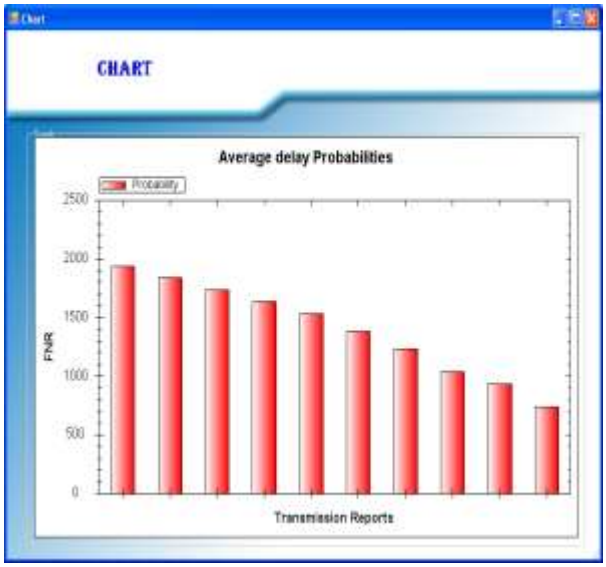


TABLE 1 COMPARISON METHODS OF FALSE DATA INJECTION

S. No	Method	Time Period	Accuracy
1.	Leach Method and LAN	3	90
2.	M-Leach Method and LAN	2.75	95
3.	Hill Climbing Method and Wi-Fi	1.25	100

Chart 2 TIME PERIOD COMPARISON

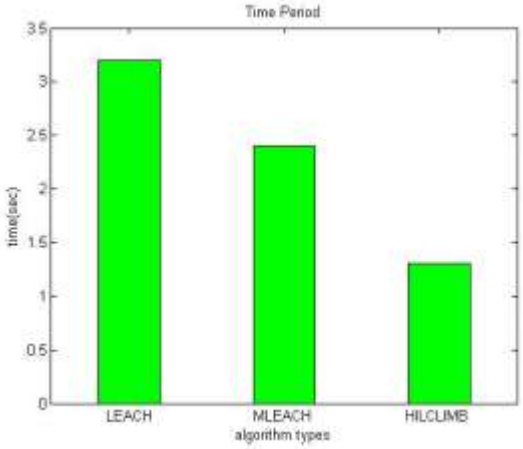
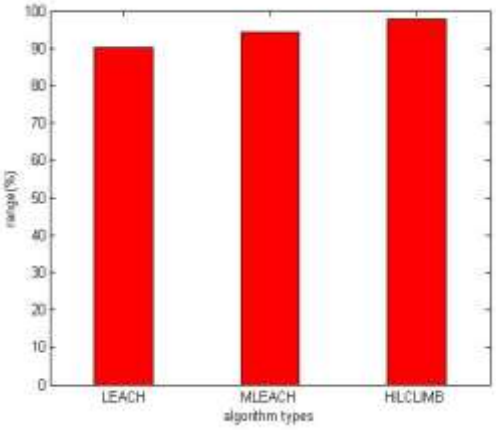


Chart 3 ACCURACY COMPARISON



V. Conclusions

A number of recent research efforts have addressed security issues such as node authentication, data secrecy and integrity. They provide no protection against injected false sensing reports once any *single* node is compromised. Our analysis and simulation results show that SEF can effectively detect false reports even when the attacker has obtained the security keys from a number of compromised nodes, as long as those keys belong to a small number of the key pool partitions. SEF represents a first step towards building resilient

sensor networks that can withstand *compromised* nodes. SEF achieves this goal by carefully limiting the amount of security. Information assigned to each individual node.

The future enhancement of Co-operative Bit-Compressed Authentication (CBA) scheme for false data injection and preventing the compromised node attacks had been analysed by the theoretical analysis. It is observed from the experiments that the BECAN scheme can achieve better en-routing filtering probability and improved reliability with multi-reports. The performance of the packet delivery ratio, end-to-end latency and throughput of the proposed system are achieved in the simulation experiments. The BECAN method can be used to other mechanism it can prevents the unauthorized user to access through the false data injection attacks from the mobile compromised sensor nodes through the routing protocols.

ACKNOWLEDGMENT

We the authors of this paper thank our institution for the support and encouragement given to undertake the research work. We also thank the authors of the reference papers used to carry out this research work.

REFERENCES

[1].F. Ye, H. Luo, S. Lu, and L. Zhang, "*Statistical En-Route Detection and Filtering of Injected False Data in Sensor Networks*," IEEE INFOCOM '04, Mar. 2004.

[2].Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui Liang, and Xuemin (Sherman) Shen, "*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, January 2012.

[3].Teenu Liza Thomas and P. Vijayalakshmi "*Cooperative Bit-Compressed Authentication Scheme against Compromised Node Attacks in Wireless Sensor Networks*" International Journal of Computer Applications (0975 – 8887) Volume 71– No.19, June 2013 .

[4].H. Yang and S. Lu. "*Commutative cipher based en-route filtering in wireless sensor networks*". In Vehicular Technology Conference, 2004.VTC2004 Fall.2004 IEEE 60th, volume 2, pages 1223-1227.IEEE, 2004.

[5].C. Kraub, M. Schneider, K. Bayarou, and C. Eckert. "Stef: *A secure ticket-based en-route filtering scheme for wireless sensor networks".* In Availability, Reliability and Security, 2007. ARES 2007.The Second International Conference, pages 310-317. IEEE, 2007.

[6].Z. Yu and Y. Guan." *A dynamic en-route filtering scheme for data reporting in wireless sensor network"s*. IEEE/ACM Transactions on Networking (ToN), 18(1):150-163, 2010.

[7].K. Ren, W. Lou, and Y. Zhang, "*Multi-User Broadcast Authentication in Wireless Sensor Networks*," Proc. IEEE Sensor Ad Hoc Comm. Networks (SECON '07), June 2007.

[8].Nithya Menon, S.Praveena *"BECAN: A Bandwidth Efficient Cooperative Authentication Scheme for Wireless Sensor Networks*" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-6, May 2013.

[9].Akylidz.J, Weilian Su,Boyen.X (2003*)"A Survey on Wireless Sensor Networks". IEEE Communication Magazine 2002* , LNCS, Vol.2729, pp. 383399, Springer-Verlag,.

[10].www.ijarcce.com/ "Projective *Clustering Approach for the Detection of Outlier and Non- Axis-Aligned Subspaces".*

[11].https://prezi.com/t6aixt0sdx9/

[12].https://en.wikipedia.org/wiki/Link_aggregatin

[13].Dong.J, Chen.Q, and Niu.Z, (2007) "*Random Graph Theory Based Connectivity Analysis in Wireless Sensor Networks with Rayleigh Fading Channels*," Proc. Asia-Pacific Conf. Comm. (APCC '07),pp. 123-126.

[14].Chen.J, Yu.Q, Zhang.Y, Chen.H, and Sun. Y, (2010) *"Feedback Based Clock Synchronization in Wireless Sensor Networks: A Control Theoretic Approach*," IEEE Trans. Vehicular Technology, vol.59, no. 6, pp. 2963-2973.

[15].W. Mao, "*Modern Cryptography:" Theory and Practice.* Prentice Hall PTR, 2003.

[16].Zhu, Zhengjian, Qingping Tan, and Peidong Zhu. *"An effective secure routing for false data injection attack in wireless sensor network."* In Managing Next Generation Networks and Services,pp.457-465.Springer,2007.

[17].V.M.Sivagami, K.S.Easwara Kumar "*False Data Detection Using MAC pairs in Wireless Sensor Networks"International Journal of Computer Trends and Technology (IJCTT)*,V4(4):539-545 April Issue 2013 .ISSN 2231-2803.www.ijcttjournal.org. Published by Seventh Sense Research Group.

[18].Mrs.P.Radhadevi, D Gopi Krishna *"Clone Attacks Detection In Wireless Sensor Networks"International Journal of Computer Trends and Technology (IJCTT)*,V4(6):1527-1529 June Issue 2013 .ISSN 2231-2803.www.ijcttjournal.org. Published by Seventh Sense Research Group.