I J C T A, 8(5), 2015, pp. 2285-2292
© International Science Press

EEGA: Energy Efficient Group Authentication for detecting DoS attacks in Wireless Sensor Networks

Jerine S.* and Julia Punitha Malar Dhas**

Abstract: Wireless Sensor Network (WSN) contains small sensor nodes with limited computational and communication capabilities. Mainly it is used for monitoring the environmental conditions such as temperature, vibration, noise, pressure, movements etc. Wireless Sensor Network is vulnerable to many types of attacks such as wormholes, selective forwarding and Sybil attacks, because of the disseminated nature of sensor nodes. In this kind of network, authentication is crucial for secure data transmission and also to identify wrong access requests from unauthorized users. In this paper we propose an energy efficient group authentication (EEGA) mechanism to perceive DoS attacks. Our method identifies DoS attack by filtering the injected false data using MAC (Message Authentication Code). The proposed EEGA scheme can save sensor nodes energy by timely identifying and filtering the majority of false data with minimal operating cost at the routing nodes. So that only few number of injected false data needs to be checked by the sink, which thus minimizes the burden of the sink. Performance evaluation shows the effectiveness of the proposed EEGA scheme in terms of high filtering probability and energy saving.

Key Words: Wireless Sensor Network, Authentication, Filtering false data, Message Authentication Code.

1. INTRODUCTION

A Clustered Wireless Sensor Network is composing of large number of sensor nodes, Cluster Head, and a sink node. These nodes are interconnected to execute distributed sensing tasks. Each sensor node is low cost but has required sensing, processing and communicating components. As a result, when a sensor node generates a message will be reported through cluster head and routing nodes to the sink node [1] [2].

Wireless Sensor Networks are typically set up in unattended environment. Therefore they are susceptible to many types of attacks such as selective forwarding, Sybil and wormholes attacks [3][4].It may also be affected by false data attack [5]. In this, the sensor nodes are first compromised by the adversaries and use them to send bogus messages to the sink node which causes high level error decision and energy wastage in the routing nodes. It is not easy to identify the inserted false data exactly in wireless sensor networks. Concurrent transmission of false data to the sink node not only causes energy wastage but also requires deep verification functions. Therefore injecting false data should be executed in both routing nodes and in sink node. For this many false data filtering mechanisms were developed [6][7][8]. Most of the existing mechanisms use symmetric key cryptography. According to this once the attacker hacked the secret key then the consistency of the filtering mechanism will be degraded.

This paper proposes an energy efficient group authentication (EEGA) scheme for identifying the DoS attacks by filtering false data in wireless sensor networks. When comparing with the earlier schemes, this EEGA scheme provides high filtering probability and high reliability.

* Research Scholar, Department of Computer Applications, Noorul Islam University, Kumaracoil, Thuckalay, K.K.Dist-629180, Tamil Nadu, India, *Email: ssjerine@gmail.com*

** Professor & Head, Dept of Computer Science and Engg, Noorul Islam University, Kumaracoil, Thuckalay, K.K.Dist-629180, Tamil Nadu, India, *Email: julaps113@yahoo.com*

The rest of the paper is organized as follows. Section 2, reviews some related works. Section 3, introduces the system model and design goal. Section 4, presents the proposed EEGA scheme. Section 5, analyzes the results and performance, and finally section 6 concludes the paper.

2. RELATED WORK

Recently many research works were developed in wireless sensor network for filtering the injected false data attack. In [1], Rongxing et al proposes a novel bandwidth efficient cooperative authentication (BECAN) scheme for filtering injected false data in wireless sensor networks. It uses TinyECC based non interactive key pair establishment and message authentication code. Two phases nodes initialization and deployment and sensed results reporting are used n this scheme. This scheme saves energy by early detecting and filtering the majority of injected false data with minor extra overheads at the en-route nodes. In addition, only a very small fraction of injected false data needs to be checked by the sink which largely reduces the burden of the sink. In [3], Ren et al. propose a more efficient location aware end to end data security design (LEDS) to provide end to end security including false data filtering capability. In [5], Zhu et al. present an interleaved hop by hop authentication (IHA) for filtering false data. In IHA each node is associated with two other nodes along the path, one is the lower authentication node and other is the upper authentication node. An en-route node will forward the data if it is successfully verified by its lower authentication node. In [8], Ye et al. developed an algorithm called SEF for filtering the false data. In this, multiple keyed message authentication code (MAC) is used to validate sensed information. It uses random subset of keys to verify the MAC. Also to save bandwidth it uses bloom filter. In [9], Yang et al. proposed a Location Based Resilient Secrecy (LBRS), which adopts location key binding mechanisms to reduce the damage caused by node compromise and further mitigate false data generation in wireless sensor networks. In [10], Zhang et al. provide a public key based solution to en route filtering. It uses private keys to bind the location based keys. In [11], Anjali et al. suggested an Identity based signature scheme for efficient batch verification of multiple signatures to mitigate gang injection of false attack threat. It allows any pair of users to communicate securely and to verify each other’s signatures without exchanging public key certificates. In [12], Vimala et al. proposed a cooperative authentication scheme for filtering the false data injection by set of adversaries. It also uses Virtual Backbone Scheduling (VBS) scheme to save energy in sensor nodes by turn off their radios having low energy. In [13], Uma et al. formulated CAFS which filters false data. CNR based MAC code technique used in this scheme saves energy by early detecting and filtering the majority false data with less overhead.

3. SYSTEM MODEL AND DESIGN GOAL

This section formulates the network model, the security model and identifies the design goal of the proposed EEGA scheme.

3.1. Network Model

We consider a clustered wireless sensor network which consists of number of sensor nodes $SN = \{SN_0, SN_{1, \ldots\ldots\ldots}\}$, Cluster Heads (CH), and a sink node. Sensor nodes are set up at random in the area A. The sink is a dominant node for data collection computation and storage. The sink node is responsible for initializing the sensor nodes. A unique identifier is given to all sensor nodes for identification purpose. Communication is bidirectional ie, sensor nodes inside the communication range(R) may communicate with every other. Sensor nodes can forward data via established route through the cluster heads. So such undirected graph $G = \{V, E\}$ be proficient to be used to represent such type of wireless sensor networks, where $V = \{V_1, V_2, \ldots\ldots\ldots\}$ is the set of sensors $SN = \{SN_0, SN_1, \ldots\ldots\ldots\ldots\}$and a sink node, E = $\{(V_i, V_j) \mid V_i, V_j € V\}$is the set of edges, $d(V_i, V_j)$ is the distance between two nodes V_i, V_j . An edge e_{ij} indicates whether there exists a communication link between nodes V_i and V_j or not is defined as,

$$e_{ij} = \begin{cases} 1, d(V_i, V_j) \leq R \\ 0, d(V_i, V_j) > R \end{cases}$$

3.2. Security Model

If a wireless sensor network is insecure, malicious adversaries may launch security attacks to degrade the network functionalities. Attackers can send false data that floods into the sink then the sink will be surely affected by DoS attack. Therefore our model focuses on detecting the false data injected by malicious node.

3.3. Design Goal

The design is to develop an energy efficient group authentication scheme for identifying the false data injected in the wireless sensor networks.

4. PROPOSED EEGA SCHEME

This paper proposes an energy efficient group authentication scheme to filter false data that were injected by compromised nodes in clustered wireless sensor networks. This scheme uses MAC (Message Authentication Code) to provide data confidentiality. It also uses neighbor nodes and routing nodes to ensure efficient filtering of false data and end to end delivery of messages to the sink node.

In the proposed scheme each sensor node in the cluster is initially loaded with a master key and each sensor is mutually authenticated by its cluster head (CH). Before forwarding the sensed data, it is authenticated by the neighbor nodes. For that a secret key domain {K_1, K_2…..} is created by cluster head (CH) and distributed to all cluster members to generate MAC. The generated MAC code is aggregated into a vector by the source node and forwarded to base station via cluster head and routing nodes is shown in Fig 1.

This vector is verified by the routing nodes in the conventional path, if the sensed data is valid then it is forwarded to sink node. The sink node also verifies the received MAC to identify false data.

Our proposed EEGA scheme is divided into three phases: Node initialization and key distribution, MAC generation, and MAC verification.

The work flow of the proposed scheme is shown in Figure 2,

4.1. Node Initialization and key distribution

The sensor nodes are generally installed in unattended environment. Each sensor node is initially loaded with an identifier and a master key. Sensor nodes are initialized by invoking algorithm 1. After each sensor

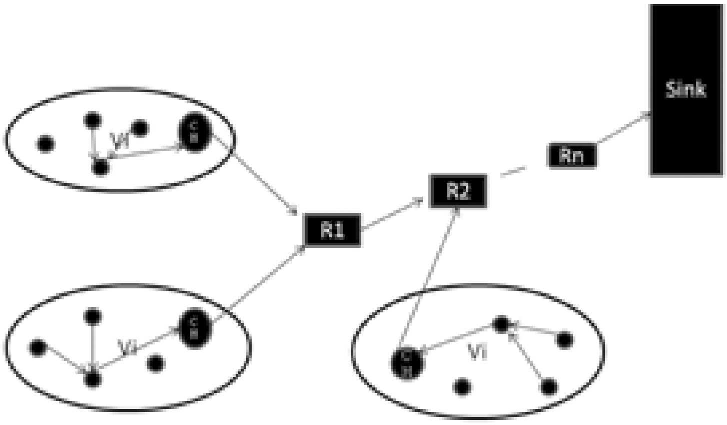

Figure 1: Group Authentication Architecture

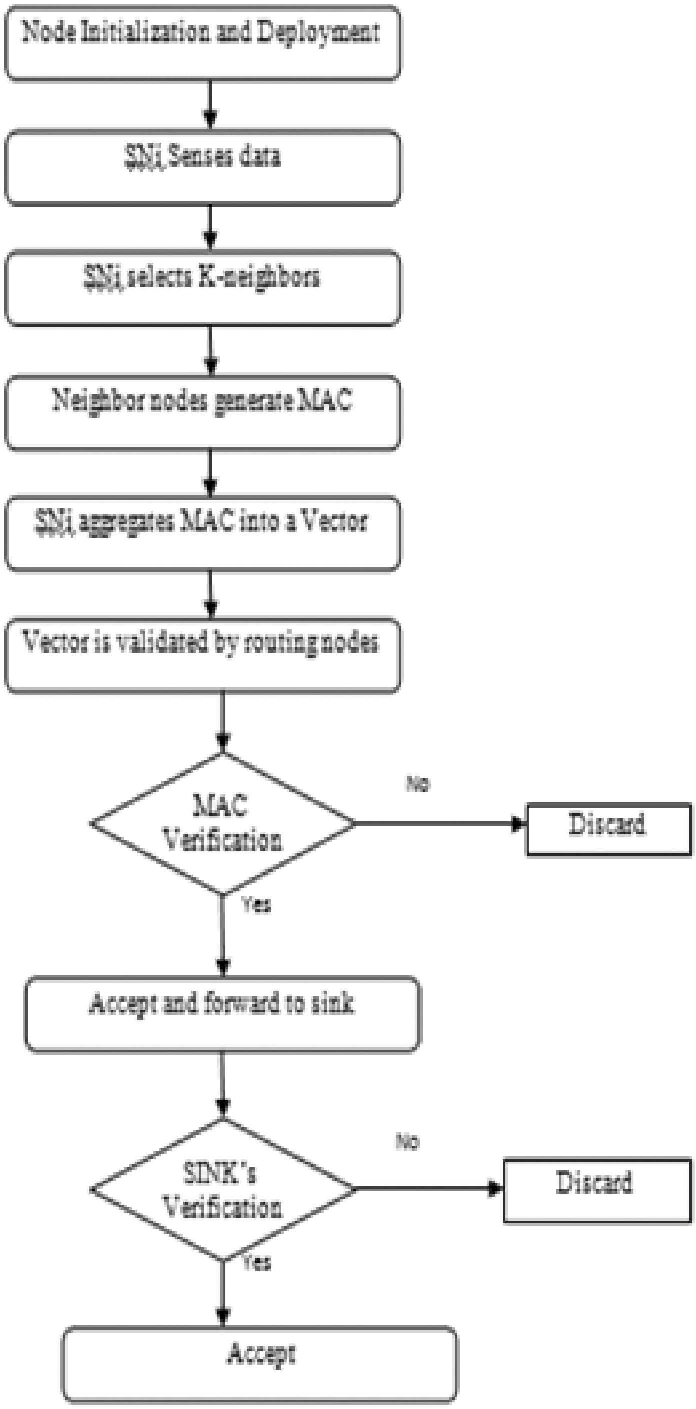
Node Initialization and Deployment
SNi Senses data
SNi selects K-neighbors
Neighbor nodes generate MAC
SNi aggregates MAC into a Vector
Vector is validated by routing nodes
MAC Verification
No
Discard
Yes
Accept and forward to sink
SINK's Verification
No
Discard
Yes
Accept

Figure 2: Flowchart of proposed scheme

node is initialized it is mutually authenticated by cluster head, which generates a key domain for its members. Using this key domain sensor node can make communication with its neighbors in the transmission range.

```
Algorithm 1. Node Initialzation and Key Establishment
Input:   {id, master key}, $SN = \{SN_0, SN_1, \ldots\}$
Output:  Secret key domain $K = \{K_0, K_1 \ldots.\}$.
 1. For each node $SNi$ € $N$ do
    Preload $SNi$ with $id$ and master key
```

```
2. Mutually authenticate $SNi$ by CH
3. Generate secret key domain($Ki$)
4. End for
5. Return secret key domain ($Ki$)
```

4.2. MAC Generation

When a sensor node *SNi* is ready to transmit message (*Mi*), it attaches current timestamp and selects *K* neighbors to generate $mac_{i.}$. source then group together generated mac_i into a vector (*Vi*) and is forwarded through $CH \rightarrow R1 \rightarrow R2 \ldots\ldots \rightarrow R\text{i} \rightarrow BST$. Algorithm 2 is used for generating $mac_{i\ .}$

```
Algorithm 2. MAC Generation
Input:    $SNi$, $NNi$, $mi$, $T$
Output:   MAC
1. $SNi$ computes shared key $Kij = \{Ki1, Ki2\ldots\ldots\}$ with each node in the neighbor
2. If $SNi$ believes the message $mi$ is correct then
3. For $j = 1$ to $n$ do
       $mac_{ij} = MAC(m_i||T, Kij)$
4. Else
       $Mac_{ij}$ = random bit
5. Return $MAC = (mac_{i1,}\ mac_{i2}\ldots..)$
```

4.3. MAC Verification

The generated $MAC = (mac_{i1,}\ mac_{i2}\ldots..)$ is then forwarded through established routing nodes $RN_{i.}$. When a routing node R_i receives ($m_{i,}\ T$, *MAC*) it invokes Algorithm 3 for verification. If the algorithm returns "true" then it forwards the message to next node otherwise it immediately discards the message.

```
Algorithm 3. MAC Verification
Input:    $RN_i$, $m_{i,}\ T$, $MAC$
Output:   true or false
1. Set returnvalue = "true"
2. For $i$ =1 to $k$ do
       $\text{mac}_{ij}$ ‡ = MAC ($m_i||T, Kij$)
3. if $mac_{ij}$ X|OR $mac_{ij}$ ‡ $\neq 0$ then
4.  Set return value = "false"
5.  Break
6. Return returnvalue
```

5. PERFORMANCE EVALUATION

This section evaluates the performance of proposed EEGA scheme using filtering ratio, transmission delay and data reporting rate.

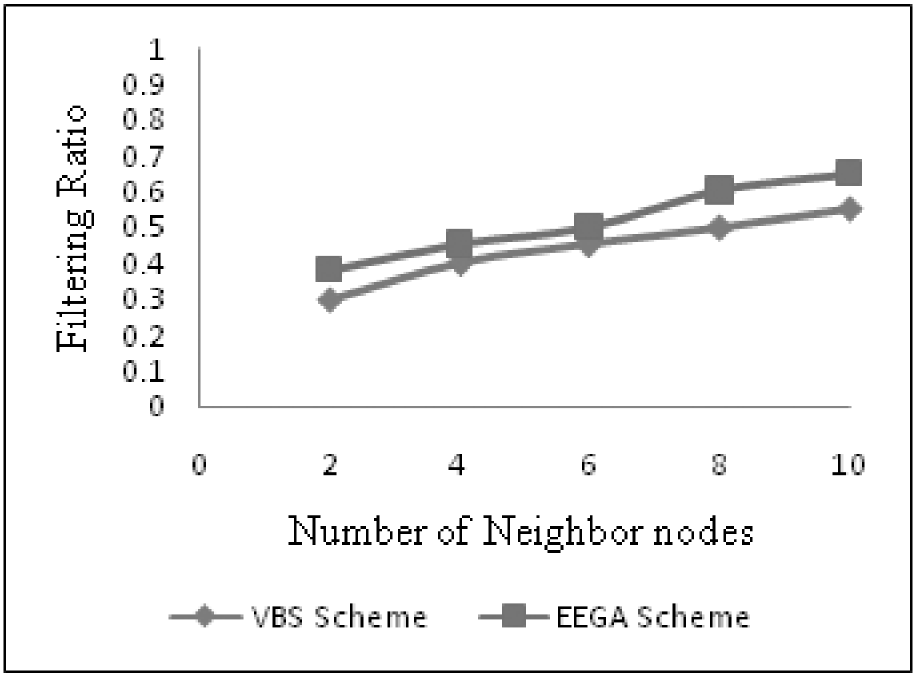

Figure 3: False data filtering ratio

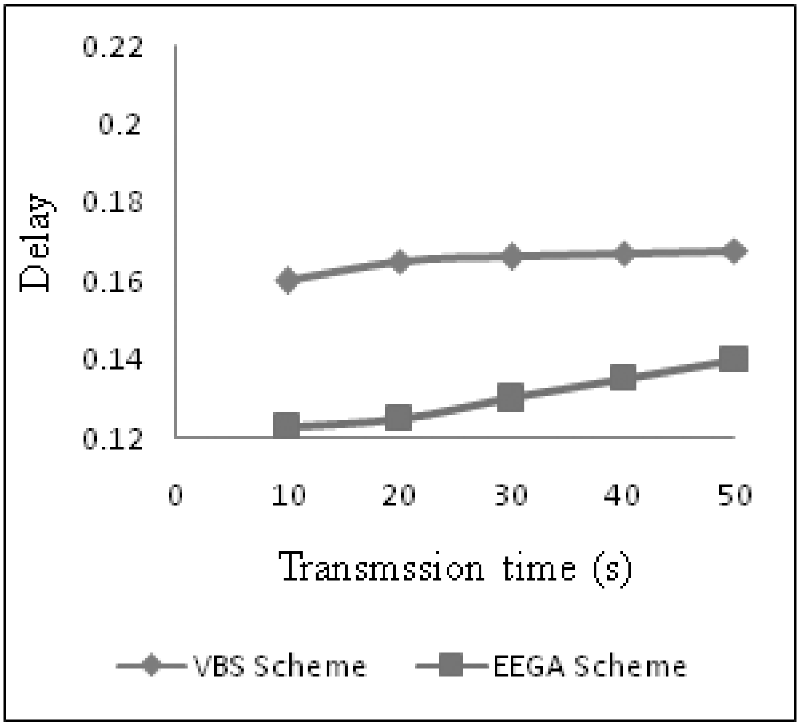

Figure 4: Transmission Delay

5.1. Filtering ratio

$$\textbf{Filtering ratio} = \frac{\textbf{Number of true packets}}{\textbf{Total number of packets}}$$

Figure 3 shows the filtering ratio of proposed scheme. The proposed EEGA scheme uses group authentication to filter the injected fake data in wireless sensor network. It uses K number of neighbor nodes to authenticate the data. When the number of neighboring nodes increases, the filtering ratio will

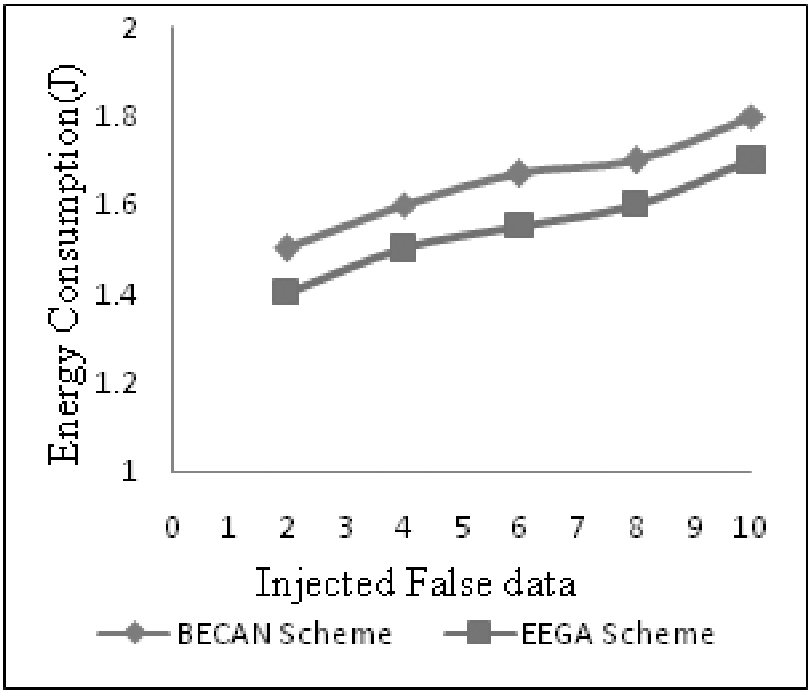

Figure 5: Energy Consumption

also increase, because when a compromised node sends false data to sink it can be filtered by at least one uncompromised node in the routing.

5.2. Transmission delay

Delay = (Arrival time-sending time)

The existing VBS scheme has high transmission delay because of complex authentication function such as Tiny ECC based non interactive key pair establishment. But the proposed EEGA scheme in this paper uses simple authentication functions which needs less verification requirements thus automatically reduces transmission delay is shown in Figure 4.

5.3. Energy Consumption

Figure 5, shows the energy consumption of BECAN and our EEGA scheme. Complex algorithms in BECAN need more computation. So energy consumption is high in BECAN. But the proposed EEGA scheme uses simple authentication function which needs less energy.

6. CONCLUSION

Due to the limited capability of a Sensor node, it is difficult to prevent the sensor nodes from DoS attack. DoS detection mechanism used in wireless networks are not suitable for Wireless Sensor Network because of limited energy and lack of management. In this paper, we have proposed an energy efficient group authentication (EEGA) scheme for detecting DoS attacks by filtering injected false data in wireless sensor networks. Performance analysis shows that the proposed EEGA scheme provides high reliable data transmission using MAC. Due to simple and energy efficiency this scheme is well suits to wireless sensor networks.

References

[1] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Xiaohui Liang, Xuemin Shen,”BECAN: A Bandwidth Efficient Cooperative Authentication Scheme for Filtering injected false data in wireless sensor networks”, IEEE Computer Society, 2012.

[2] K. Akkaya and M. Younis, "A Survey on Routing Protocols for Wireless Sensor Networks," Ad Hoc Networks, vol. 3, no. 3, pp. 325-349, May 2005.

[3] K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks," Proc.IEEE INFOCOM '06, Apr. 2006.

[4] V.C. Giruka, M. Singhal, J. Royalty, and S. Varanasi, "Security in Wireless Sensor Networks," Wireless Comm. and Mobile Computing, vol. 8, no. 1, pp. 1-24, Jan. 2008.

[5] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004.

[6] L. Zhou and C. Ravishankar, "A Fault Localized Scheme for False Report Filtering in Sensor Networks," Proc. Int'l Conf. Pervasive Services, (ICPS '05), pp. 59-68, July 2005.

[7] Z. Zhu, Q. Tan, and P. Zhu, "An Effective Secure Routing for False Data Injection Attack in Wireless Sensor Network," Proc. 10th Asia-Pacific Network Operations and Management Symp.(APNOMS '07), pp. 457-465, 2007.

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

[9] H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward Resilient Security in Wireless Sensor Networks," Proc. Sixth ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc '05), pp. 34-45, 2005.

[10] Y. Zhang, W. Liu, W. Lou, and Y. Fang,"Location-Based Compromise-tolerant Security Mechanisms for Wireless Sensor Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 247-260, Feb. 2006.

[11] Anjali Thampi, Nithya," An efficient ID based scheme for filtering gang injected false data in wireless sensor networks", IJARCCE, Vol 2, ISSN:2319-5940, 2013.

[12] D.Vmala, Srinivasan, Vinoth, Arun Prasath," Protection of wireless sensor network from gang injected false data attack", IJAREEIE, Vol 1, ISSN:2320-3765, 2014.

[13] Uma Narayan, Arun Soman, "CAFS: Cluster based authentication scheme for filtering false data in wireless sensor networks", IJARCCE, ISSN: 2319-5940, 2013.