ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2014

Protection of Wireless Sensor Network from Gang Injecting False Data Attack

D.Vimala[1], R.Srinivasan[2], R.Vinoth[3], D.Vinoth [4], M.M.Arun Prasath[5]

Asst. Professor, Dept of EEE, PGP College of Engg & Tech, Namakkal, Tamilnadu, India[1]
Asst. Professor, Dept of EEE, Muthayammal College of Engg, Rasipuram, Tamilnadu, India[2]
Asst. Professor, Dept of ECE, Muthayammal College of Engg, Rasipuram, Tamil Nadu, India[3]
Asst. Professor, Dept of EEE, Muthayammal College of Engg, Rasipuram, Tamil Nadu, India[4]
Asst. Professor, Dept of ECE, Annapoorana Engineering College, Salem, Tamil Nadu, India[5]

ABSTRACT: Gang injecting false data attack is a serious threat to wireless sensor network (WSN), for which an adversary reports false information to sink, causing high overload and energy waste in en-route nodes. In this paper, we propose a Co-operative authentication scheme used for filtering the false data injected by a set of adversary and Virtual Backbone Scheduling (VBS) scheme is used to save energy in sensor nodes by turn-off their radios having low energy. In the proposed scheme, the overload occur in sink can be reduced by early detecting and filtering gang injected false data. Both theoretical and simulation results are given to demonstrate the effectiveness of the proposed scheme in terms of high filtering probability and energy saving.

KEYWORDS: False data attack, Co-operative authentication, Virtual backbone scheduling.

I. INTRODUCTION

A wireless sensor network (WSN) consists of collection of sensor nodes and a sink (Base Station). The sensor nodes are placed in certain interest region (CIR) and connected via wireless links to perform distributed sensing tasks; each sensor node performs sensing, processing the data and communicating with other sensor nodes. Therefore, when a special event occurs e.g. wild fire event, it will send the report to sink via established routing path, finally the sink process the report to take necessary actions.

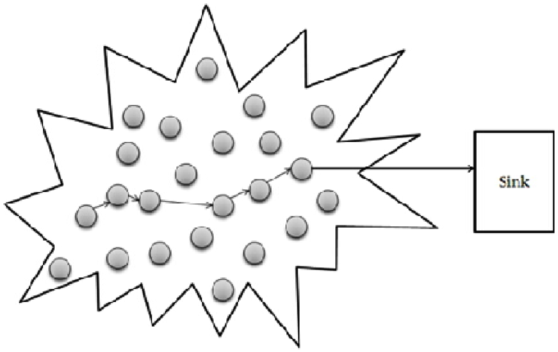


Fig. 1. A wireless sensor network under consideration (The sensor report send to sink is shown by arrow).

The above figure shows the sensors send the report to sink via established routing path. Wireless sensor networks are placed in unattended or hostile environments. The sensor nodes are low cost devices, since it is easily attacked by an adversary. For an gang injecting false data attack an adversary first compromises several sensor nodes, accesses all keying materials stored in the compromised nodes and finally the compromised nodes inject bogus information and send false data to sink. This will lead to DOS attack on sink. Sensor nodes are usually battery driven, an efficient utilization of power is essential in order to use networks for long duration, hence it is needed to reduce data traffic inside the sensor networks, reduced amount of data that need to send to sink. Therefore, energy efficiency becomes critical. The radio consumes a major portion of the energy [2]. To tackle this challenge issue, some false data filtering mechanisms have been developed, and the sensors lifetime can be maximized by backbone scheduling.

In this paper, a Co-operative authentication scheme is used for filtering gang injected false data in wireless sensor networks and the Virtual backbone Scheduling scheme is used for energy saving in sensor nodes. The main contributions of these paper are,

First, Initialize all sensor nodes and perform Co-operative authentication with its neighbors.

Second, the proposed scheme can early detect and filter the Gang injected false data in wireless sensor networks and to prevent sink from Dos attack.

Third, the virtual backbone scheduling scheme is used to save energy in sensor nodes by turn off their radio's when the nodes having low energy levels.

II. MODEL AND DESIGN GOAL

In this section, we formulate the network model, Security model and The Design goal.

A. Network Model

In network model, we consider a set of wireless nodes $N = \{N_0, N_1, N_2\ldots\}$ and sink S are placed in certain interest region with area L. The sink is a powerful data collection device, it is interconnected through the network. The communications between the two sensor nodes are bi-directional. Each sensor node $Ni \in N$ is stationary in location. Every node can be identified with its unique identifier assigned by sink. Sensor node will generate the report when any event occurs. Such as temperature change, the sensor node closer to sink will directly communicate with sink, if the sensor node is far away from the sink, it schedule the nodes to form a backbone to sink. Finally, the source node runs routing algorithm to identify the shortest path to sink through selected backbone nodes.

B. Security Model

Wireless sensor nodes are placed in unattended or hostile environments, in which, an adversary can compromise the sensor nodes to inject bogus information to sink. Therefore, in our security model, an adversary A can compromise a set of sensor nodes and obtain their all stored keying materials. Then the compromised nodes can launch some injected false data attacks and finally the sink will suffer from Dos attack. In this paper the Elliptic curve cryptography (ECC) and Message authentication code (MAC) is used for secure communication between the two sensor nodes.

C. Design Goal

The design goal is to develop a Co-operative authentication scheme for filtering gang injected false data in wireless sensor network and Virtual backbone scheduling scheme is used for maximizing the sensor lifetime, specifically, the following two desirable objectives will be achieved.

1. Early detecting and filtering injected false data by Co-operative authentication scheme.

The sink is a central data collection device, when a compromised sensor node can inject false data to sink, the sink will lead to Dos attack. In order to avoid the Dos attack, each node in wireless sensor network can share the authentication tasks with its neighbors. This scheme is used to detect and filter the false data earlier in en-routes.

2. Maximizing Sensors Lifetime

In Virtual backbone scheduling (VBS) scheme uses backbone scheduling with duty cycling for power management, VBS form multiple backbones by nodes having higher energy level. In VBS, data traffic is only forwarded by backbone sensor nodes, and the rest of sensor nodes turn off their radios to save energy (not completely turned off, Sensors kept in sleep mode).The rotation of multiple backbones makes sure that the energy consumption of all sensor nodes is balanced. The frequent turn off and turns on modes are known as sensors duty cycle.

III. PRELIMINARIES

A. Elliptic curve cryptography

Elliptic curve cryptography (ECC) is a public key cryptography used in many wireless sensor applications. ECC is suitable for wireless sensor networks to provide convenient authentication and pair key establishments.

Analog of Diffie Hellman key exchange: For any two sensor nodes A and B can be accomplished as follows:

1. A selects an integer *xi* less than n. this is A's private key. A Then generates public key $Y_i = x_i * G$; the public key is a point in eq (a, b).where G is a base point function
2. B similarly selects a private key *xj* and computes a public key Y_j.
3. A generates the secret key $k_{ij} = x_i * Y_j$.
   B generates the secret key $k_{ij} = x_j * Y_i$.

The two calculations in step 3 produce the same result because

$$x_i * Y_j = x_i * (Y_j * G) = x_j * (x_i * G)$$
$$= x_j * Y_i$$

Because of the hardness of ECC Discrete Logarithm (ECDL), only A and B can secretly share a key. If a sensor node A is compromised, then the key k_{ij} shared between B and another sensor node B' is not affected.

1. Elliptic curve encryption and decryption

For an encryption/decryption, system requires a point G and an elliptic group Eq (a, b) as parameters. Each node A selects a private key x_i and generates a public key $Y_i = x_i * G$.To encrypt and send message P_m to node B, A chooses a random positive integer K and produces the cipher text Cm consisting of the pair of points:

$$Cm = \{KG, P_m + KPB\}$$

To decrypt the cipher text, B multiplies the first point in the pair by B's secret key and subtracts the result from the previous equation

$$=P_m + KPB - xj\ (KG)$$
$$=P_m + K\ (nBG) - nB\ (KG)$$
$$=P_m.$$

B. Message Authentication Code (MAC)

Message Authentication is a mechanism or service used to verify the integrity of a message.MAC uses shared secret key. This technique assumes that two communicating parties share a common secret key K. When node A has a message to send to B, it calculates the MAC.

$$MAC = H\ (K \,||\, M)$$

Where,

M=Input message
H=Hash code
K=Secret Key

Calculated MAC and message are transmitted to the receiver. The receiver performs the same calculation on received message. Received MAC is compared with the calculated MAC. If both match then

1. The receiver is assured that the message has not been altered.
2. The receiver is assured that the message is from the alleged sender.
3. If the message includes a sequence number, then the receiver can be assumed of the proper sequence because an adversary cannot successfully alter the sequence number.

C. Virtual Backbone Scheduling with Routing (VBS)

The virtual backbone scheduling is a combined method of backbone scheduling and Duty cycling. It is a novel sleep scheduling technique, for which data traffic is only forwarded by backbone sensor nodes in wireless sensor network and the rest of sensor nodes turn-off their radios to save energy. The sensor node power consumption consists of three parts they are, Sensing, Computing and Radio. For a typical sensor node, the radio is the most power-consuming part and may even dominate the energy consumption. Therefore scheduling the radio part is an important activity in power management. The backbone nodes should be formed by sensors energy level. Each sensor node consumes a fixed amount of energy *e* in each round when working as a backbone node. A virtual node that corresponds to a sensor node as a node contains *e* energy.

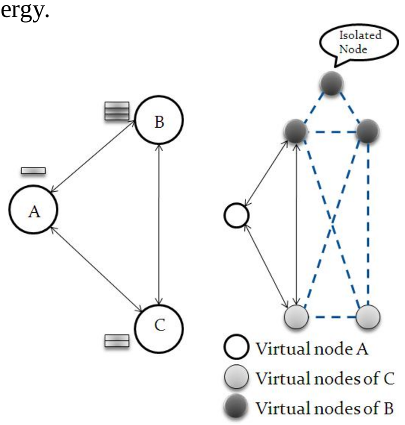


Fig. 2. The virtual nodes of different ancestors are connected with an increasing index order. As a result, virtual node 2 of a sensor node B is isolated because it has more energy and cannot be connected to the virtual nodes of A or C.

The original node is known as ancestor. An ancestor having E_r energy is divided into $[E_r/e]$ virtual nodes. The virtual nodes in same ancestor form a virtual group. In Fig. 2, the ancestor node B having 3 units of energy levels, it should be divided into 3 virtual nodes, similarly ancestor node C having 2 units of energy levels; it can be divided into 2 virtual nodes. Multiple virtual nodes in same ancestor forms virtual group. In Fig.2 the ancestor node B can be selected as backbone node because there is one isolated virtual node in ancestor B, it has more energy and cannot be connected to the virtual nodes of A or C. Then the ancestor node C will be turned off their radio to save energy. After selecting the backbone nodes, if the multiple backbone nodes having equal energy level, the source node A runs shortest path algorithm to identify shortest path to sink among the selected backbone nodes. Other remaining selected nodes are turned off to save energy.

IV PROPOSED SCHEME

In this section, we will propose Cooperative authentication scheme for filtering gang injected false data in wireless sensor networks and Virtual backbone scheduling scheme is used for maximizing sensors life time. Before proceeding the proposed scheme, the design rationale is introduced.

A. Design Rationale

To filter the false data injected by compromised sensor nodes, the cooperative authentication scheme adopts cooperative neighbor *x* router (CNR) based filtering mechanism with virtual scheduling. As shown in Fig. 3, in the CNR based authentication mechanism, when a source node N0 detects some event, then the report m is transferred to sink via established routing path through scheduling of nodes.

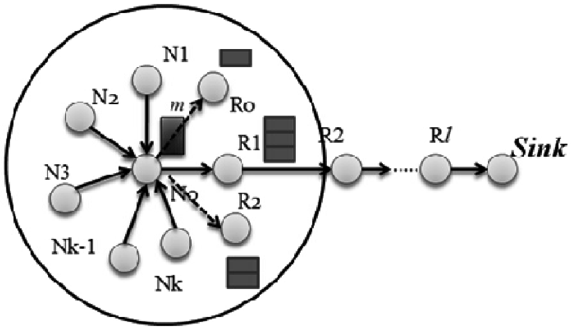


Fig. 3. Cooperative CNR based authentication mechanism

The routing path is defined as R_{N0}:{R_1,R_2…R_l,*Sink*},it first resorts to its neighboring nodes to cooperatively authenticate the report m, and then sends the report m and MAC code from N_0 U N_{N0} to the sink via routing R_{N0},where each node MAC value is calculated and the MAC value is represented in matrix.

$$\mathbf{MAC=}\begin{pmatrix} mac01 & \dots & mac0l & mac0s \\ mac11 & \cdots & mac1l & mac1s \\ \vdots & \ddots & \vdots & . \\ mack1 & \cdots & mackl & macks \end{pmatrix}$$

Where each mac_{ij}, $0<i<k$, $1<j<l$, Ni’s MAC on *m* for R_j’s authentication, and each mac_{is} represents N_i’s MAC on *m* for the sinks authentication. The sink initializes all sensor nodes; each sensor node shares its private key with the sink. According to ECC, when a compromised node sends a false data to the sink, the false data can be filtered if there is at least one uncompromised neighboring node participating in reporting. Thus the false data can be detected and filtered earlier. The probability of *k* neighbors is discussed in [1].

B. Description of proposed scheme

The proposed scheme consists of four phases: sensor node initialization, event reporting, Virtual scheduling graph, and en-route filtering & Sink Verification.

1. Sensor Node Initialization

To initialize the sensor nodes *N= {*N_0*, N1, N2…….}*, the sink invokes the algorithm1. Then the sink assigns private key to each sensor node. We assume all the sensor nodes are static, which are immobile; therefore sensor nodes are uniformly distributed in certain interest region (CIR) after deployment. Once an event occurs, the sensor node reports its event to sink via established routing path, which it should be performed by scheduling the nodes to form a backbone or adjust their routing to sink either a shortest path adopted to some resource constraints with some existing routing protocol.

2. *Event Reporting*

When a sensor node generates a report *m* after being triggered by a special event, e.g., a wild fire event or in response to a query from the sink. It will send the report *m* to sink via backbone nodes formed by virtual scheduling, as shown in Fig.3; The following protocol steps will be executed.
Step1.The source node N_0 detects an event *m* its gains the current timestamp *T*, and chooses neighboring nodes N_{N0} : {N_1, N_2…..N_K}, and sends the event (*m*, *T*)and routing R_{N0} to N_{N0}
Step2.with (*m*, *T*) as input, each sensor node $N_i \in (N_{N0} \cup \{N_0\})$ invokes algorithm2 to generate a row authentication vector and reports Rowi to the source node N0.

$$\mathbf{Row_i = (\mathit{mac_{i1}, mac_{i2} \ldots . mac_{il}, mac_{is}})}$$

*Step*3.when N_0 believes there is no compromised node. It calculates the energy level of its neighbors through virtual scheduling, and then it selects the nodes having maximum energy. Finally it transfers the report to the selected node.

3. *Virtual Scheduling Graph*

In VSG, the source node N_0 checks the energy level of its neighbors. First it checks whether the neighbor is a compromised node or not, then finally estimates the energy level of its neighbors. The nodes having maximum energy level should be selected as backbone node and turn on their radio for forwarding the messages.

Then the nodes having minimum energy level will turn-off their radios to save energy. From the Fig. 3 the node R_1 has maximum energy level (3 units) and remaining R_0 & R_2 has minimum energy levels than R_1.The R_1 node is selected as backbone to forward the messages. Nodes R_0 & R_2 turn off their radios to save battery power. The VSG initializes algorithm3 for scheduling the sensor nodes to form a backbone.

4. *En-Route filtering & Sink Verification*

(i) *En-route Filtering:*

When each senor node R_i, (1<i<l), along the backbone node R_{N0} receives *(m, T, MAC)* from its upstream node, it checks the integrity of the message *m* using MAC value and the timestamp *T*. If the timestamp *T* is out of date, The message *(m, T, MAC)* will be discarded.otherwise,R_i invokes algorithm4.If the return value is accept, R_i will forward the message to its downstream backbone node,Otherwise,the report will be discarded.

(ii) *Sink Verification:*

Finally the sink receives the report *(m, T, MAC)*, it checks the integrity of the message m and the timestamp *T*.if the timestamp *T* is out of date the report *(m, T, MAC)* will be discarded. Then the sink collects all private keys of N_i, 0<i<k, and invokes the algorithm 5.If the return value is accept, the sink accepts and process the report,Otherwise,the sink rejects the report

V ALGORITHMS

There are five algorithms used in proposed scheme they are:

Algorithm 1 Sensor Initialization

```
procedure Sensor Node Initialization
  Input: params and un-initialized N = {N0, N1, N2,…..}
  Output: initialized N = {N0, N1, N2,…..}
  for each sensor node $N_i \in N$ do
    preload Ni with ECC, params and energy
      choose a random number $x_i \in Z_q^*$ as the private key of that each Ni node
      compute the public key $Y_i = x_i G$, where G is the base point Identifier chosen at random
```

```
        Install ($x_i$, Yi) in each Ni node
    end for
    return initialized $N = \{N_0, N_1, N_2, \ldots\}$
end procedure
```

Algorithm 2 MAC Generation

```
procedure MAC generation
    Input: params, Ni ∈ ($N_{N0}$U$N_0$), m, T, $R_{N0}$.
    Output: Rowi
    $N_i$ uses shared key with each nodes.
        If $N_i$ believes the report m is true then a neighboring node is assumed having the same ability to detect a correct
    event as the source node and judge the report m.
            for j=1 to l do
                $mac_{ij}$=MAC (m||T, kij)
            end for
                $mac_{is}$=MAC (m||T, kis)
        else
            for j=1 to l do
                $mac_{ij}$ is set as a random bit
            end for
                $mac_{is}$ is set as a random bit string of length A
    end if
    return $Row_i$= ($mac_{i1}$, maci2…$mac_{is}$)
end procedure
```

Algorithm 3 Virtual Scheduling Graph

```
procedure VSG Algorithm
int CUR_ROUND=0; (Initial State)
repeat
    for each state S on sensor $N_i$ ∈ N do
        Get the associated energy levels of S;
        Prune the resultant energy levels using    min ( )
        Select the energy level of each neighbor node $N_i$ ∈ N with the maximal and minimal energy value
        Set S’s energy level to the energy level with the maximum summation among the resultant energy levels;
            if each node Ni < S
                Select the nodes and turn-off the radio
            else
                N={SB} \\ SB-selected backbones
                for all nodes Ni\\Initial node
                if Ni adjacent to SB
                then D($N_i$)=C(SB,Ni)
                else D($N_i$)= Infty
                Loop
                  find $N_n$ not in $N_i$ such that D($N_n$) is minimum.
                  Add $N_1$ to N
                  Update D($N_i$) for all Ni adjacent to $N_n$ and not in N.
                D(Ni)=min(D(Ni),D($N_n$)+C($N_n$,Ni)) //new cost to $N_i$ is either old cost to $N_i$ or known shortest path
                cost to $N_n$ + cost from $N_n$ to $N_i$//.
                Select the node $N_i$ as Backbone node
            **Until** all nodes in N.
        **end if**
    **end for**
    CUR_ROUND = CUR_ROUND + 1;
**until** All energy levels of the state S is calculated
Return the schedule represented by the Path by
  its backbone nodes.
**end** procedure
```

Algorithm 4 Enroute filtering and Sink verification

```
**procedure** EnRoute MAC Verification
  **Input**: params, $R_j \in \{R_1, R_2..R_l\}$, m, *T*, $N_{N0}$
  **Output**: accept or reject the report
each $R_j$ uses non-interactive key pair to compute shared keys with each node in $N_i \in N$ as $k_i$.
    set returnvalue = “accept”
    **for** i=0 to k do
            $mac_{ij}$ = MAC (m||T, kij)
        **if** $\overline{mac_{ij}} \oplus mac_{ij}=0$ then
            set returnvalue= “reject”
            break
        **end if**
    **end for**
**return** returnvalue
**end** procedure
```

Algorithm 5 Sink verification

```
**procedure** Sink Verification
  **Input**: params, kis, m, *T*
  **Output**: accept or reject the report
Sink looks up all private keys of nodes $N_i \in N$ and check the integrity of the received report..
    set returnvalue = “accept”
    **for** i=0 to k **do**
            $mac_{ij}$ = MAC (m||T, $k_{is}$)
        if $\overline{mac_{ij}} \oplus mac_{ij}=0$ **then**
            set returnvalue= “reject”
            break
        **end if**
    **end for**
**return** returnvalue
**end** procedure
```

VI PERFORMANCE EVALUATION

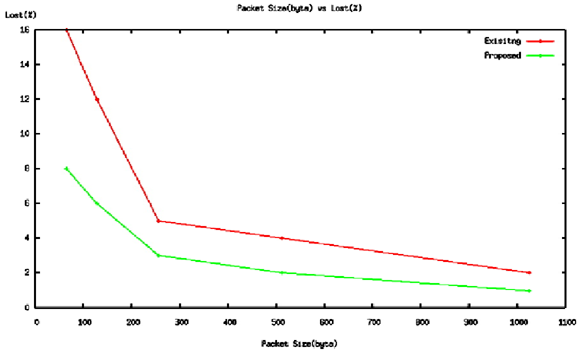
Energy saving is always crucial for the lifetime of wireless sensor networks. In this section, the performance of the proposed scheme is evaluated in terms of energy efficiency and packet loss.

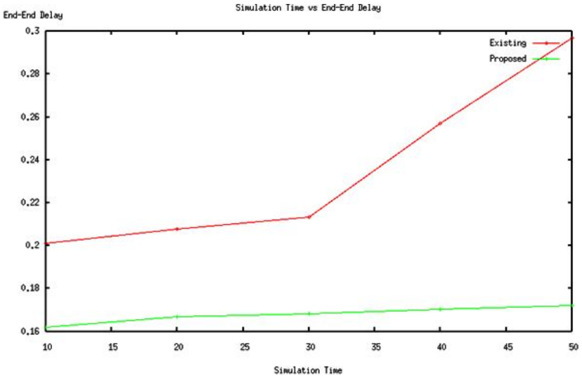
A. Energy Consumption in Key Establishments.

In proposed scheme, the additional computation costs are mainly due to Elliptic Curve Cryptography and Diffie Hellman Shared key exchange operations during the non-interactive keypair establishments. Fortunately, since keypair are distributed in each sensor node and only executed during scheduling, it wont consumes large amount of energy, because, here we use a160-bit elliptic curve for achieving the same security level as 1025-bit RSA. Assume that each sensor node is equipped with a low power high performance sensor platform. This sensor platform requires 50.81mJ to establish a shared key exchange between two sensor nodes.

B. Energy consumption during Report Transmission

In existing work [1], they deployed 200 nodes in certain interest region (CIR).All the nodes are in turn-on condition, Hence it reduces battery energy and packet loss will also occur. Sensor node which detects an event, it will report to sink via routing path. When a sensor node transfers its report to its neighbor having weak energy source, the report cannot be processed and finally the report will be discarded. The simulation results show how the existing work has more packet loss. Which it is indicated by red line in graph. The proposed scheme has better scheduling scheme to turn off their radios during nodes having reduced amount of energy level. In this scheme has better energy saving (shown in green line) compared to existing work.





Since, In existing work there should be large amount of delay during packet transmission, Because of complex authentication and routing schemes. The simulation results shows the proposed Virtual backbone scheduling scheme forms multiple overlapped backbones to transfer the packets, which work alternatively to prolong the network lifetime. The traffic is only forwarded by backbone sensor nodes, The rotation of multiple backbones makes sure that the energy consumption of all sensor nodes is balanced, which fully utilizes the energy and provides longer life time.

VII RELATED WORKS

Recently, some research works on filtering of gang injected false in wireless sensor network have been appeared in the literature in detail [1]. In [1] the proposed BECAN (Bandwidth efficient cooperative authentication) scheme is used for filtering the injected false data. Here, the bandwidth can be improved by early detecting and filtering the injected false data in en-routes. In BECAN scheme, the sensor energy should be wasted, which it will reduce the lifetime of the nodes; finally the nodes will be in dead state. This can cause a big disaster. Sensor lifetime maximization is a more important thing. Wireless sensor networks are used in most of the application such as habitat monitoring and actuating [6]. In these applications, the sensor nodes use batteries as the sole energy source. BECAN scheme does not consider the sensors lifetime. The major drawback in BECAN scheme, is packet loss during communication between the two nodes, when a source node will send a report to the weak energy sensor node via routing path, the report cannot be processed and delivered to sink.

In [2] Yeet Al. propose a stastical en-routing filtering mechanism called (SEF).SEF requires that each sensing report be validated by Message Authenticated Code (MAC).The MAC should be verified by the nodes in WSN and finally send the event to sink, finally the sink also verifies the correctness of MAC in each report and reject the false ones. Besides, SEF does not consider the possibility of en-routing nodes compromise, which is also crucial to the false data filtering.

In [3], Ren Et al, propose an efficient location aware end to end data security (LED) guarantee including efficient en-routing false data filtering capability and high level assurance on data availability. Led's is a symmetric key based solution, to achieve en-rote filtering, it requires location aware key management

Medium access control (MAC) scheme is used for power saving in WSN. In [5] Simarpreet Kaur, present an S-MAC (sensor MAC) scheme is used for saving the energy in sensor nodes. This scheme is used to solve the energy consumption related problems of idle listening, collisions and over hearing in WSNs.S-MAC considers that nodes does not need to be awake at all the time given to the low sensing event and transmission rates. The S-MAC reduces the idle listening problem by turning the radio off and on periodically, nodes are synchronized to go to sleep and wake up at the same time. The drawbacks of using S-MAC are, it does not use RTS/CTS which increases the collision probability, the main problems in S-MAC are longer listen period and sleep delay [2].

State Transition Graph (STG) is used for scheduling. In [6]. Feng Li, present an STG scheme is used for scheduling the sensor nodes in WSN.The search is start from initial state, the node states energy levels are computed from those of the starting state of transmission. Each state keeps the longer energy levels. There should be more complexity to find a path to transfer the data. A path terminates when its associated energy level is zero, when all paths terminate, the longest path is found. Which it is more complex one.

Different from above works, the proposed cooperative authentication scheme with virtual scheduling adopts an filtering mechanism to early detect and filter the gang injected false data in en-route nodes. This scheme does not require an complicated security association [1] [3]. In addition, the virtual scheduling scheme is used for maximizing the sensors lifetime by turn-off their radios, when it is not in use.

VIII CONCLUSION

In this paper, we have proposed a Cooperative authentication with Virtual backbone scheduling scheme. By theoretical analysis and simulation evaluation, the proposed scheme is used as to detect and filter the injected false data earlier in en-route nodes. This proposed scheme not only having high filtering probability but also high energy saving with virtual backbone scheduling. Finally, routing on selected backbone provides shortest path to sink for fast report transfer.

In our future work, we will investigate how to prevent the injected false data attack from mobile compromised sensor nodes.

REFERENCES

[1] Rongxing Lu, "BECAN: A Bandwidth-Efficient Cooperative Authentication scheme for Filtering Injected False Data in Wireless Sensor Networks,"IEEE transactions on Parallel and Distributed Systems, Jan.2012.

[2] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route detection and filtering of injected false data in sensor networks," in *IEEE Infocom'04*, Hong Kong, China, March 7-11 2004.

[3] K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing location-aware end-to-end data security in wireless sensor networks," in *Proc.IEEE INFOCOM 2006*, Apr. 23-29 2006.

[4] R. Szewczky, A. Mainwaring, J. Anderson, and D. Culler, "An analysis of a large scale habit monitoring application," in *ACM Sensys'04*, 2004.

[5] Simareet Kaur and Leena Mahajan, "Power Saving MAC Protocols for WSNs and Optimization of S-MAC Protocol"Intl.J. radio frequency identification and WSN, Vol. 1, Apr 2011.

[6] Feng Li and Sangulu Lu, "On Maximizing the Lifetime of Wireless Sensor Networks Using Virtual Scheduling Scheme", IEEE trans. on parallel and distri. systems, vol. 23, No. 8,Aug 2012.

BIOGRAPHY

R.Vinoth was born in Tamilnadu, India in 1985. He received B.E from Mohamed Sathak Engg College, Kilakarai,Ramanathapuram, India in the year 2007 and M.E. (VLSI DESIGN) from Muthayammal Engg College, Rasipuram, India in the year 2009. His area of interest includes image processing, Signal Processing. He is having 5 years of teaching experience in the department of Electronics and Communication Engg. He published few research papers in international journals and presented few papers in national and international conferences.