An Approach To Secure Leach Using Tesla Based Certificate

Shyamala Ramachandran[1], Valli Shanmugam[2]

[1.] Assistant Professor, Department of Information Technology, University College of Engineering Tindivanam, Melpakkam 604 001. vasuchaaru@gmail.com
[2.] Associate Professor, Department of Computer Science and Engineering, College of Engineering, Anna University, Chennai-25. valli@annauniv.edu

Abstract: Wireless Sensor Network (WSN) has a group of sensors, which communicate by hop-by-hop communication for applications like surveillances, military and tracking. The WSN has low computational power and energy. So, the algorithms designed for WSN should be such that, they extend the lifetime, use less computations with maximum coverage. Low Energy Adaptive Clustering Hierarchy protocol (LEACH) is secured in this approach. Since WSN is deployed in hostile environment, LEACH is prone to active attacks. Many attempts exist to improve the security of LEACH. This approach uses TESLA based certificate to secure LEACH. A secure head selection and secure data transfer is achieved using TESLA based certificates. Packet delivery ratio, network throughput, average network delay and energy consumption are measured. The performance metrics of secured LEACH is compared with Unsecured LEACH. The NS-2 simulator is used in implementing secured LEACH.

[Shyamala Ramachandran, Valli Shanmugam. **An Approach To Secure Leach Using Tesla Based Certificate.** *Life Sci J* 2013;10(2):1018-1027] (ISSN:1097-8135). http://www.lifesciencesite.com. 143

Keywords: LEACH, WSN, TESLA, Routing attacks, Packet delivery ratio.

1. Introduction

WSN (Akyildiz et at., 2002) consists of group of sensors linked by wireless medium and performs sensing tasks. The WSN observes the physical world, process the data, decides based on the observations and takes appropriate actions. The applications of WSN includes battle field surveillances, climate control in buildings, nuclear, chemical and biological attack detection, home automation and environment monitoring. The WSN is multi hop scalable network topology. But, it also has constraints such as, low computation and communication capability, low battery power, limited memory and sensing capability.

The WSN has hundreds or thousands of sensor nodes. These sensors communicate with each other or to an external base station (BS). When a sensor node detects an event, it records the event and routes it to the base station for further processing. The routing protocol faces challenges in selecting a best relay node within the communication range. The sensed data should be routed towards the base station in an energy efficient way. The sensor nodes in the same communication range may sense the same value. So, the relay node aggregates the data and forwards towards the base station to achieve high efficiency. Therefore, hierarchical structure with resource limited sensor nodes and high energy capacity cluster heads are preferable for WSN. Because of wireless communication, routing is prone to security threats in WSN. Therefore, the hierarchical routing of WSN should address the selection of cluster head (CH), formation of clusters, cluster adaption to mobility and resistance to security threats. The LEACH protocol (Tripathi et al., 2012) addresses all the above characteristics except security. So, this work focuses on securing LEACH using TESLA based certificates.

The rest of this paper is organized as follows. Section 2 explains the network assumption and describes how LEACH is secured using TESLA based certificates. Section 3 describes the simulation environment and analyses the performance of secure LEACH. Section 4 concludes the work.

2. Materials and Methods

Network Assumption

The network has a central base station and it is a heterogeneous network. The base station has abundant computation resources. In a heterogeneous network all the nodes have varying energy. The base station has the TESLA key, which is delayed and disclosed to all the sensor nodes. The base station acts as the trusted key distribution center (KDC). It is trustworthy and cannot be compromised. The nodes in the sensor network are resource constrained. Each node has a unique ID. The nodes communicate with each other by multi-hops. All the nodes are loosely time synchronized using the NTP protocol. The clock difference between any two nodes does not exceed the error rate (Δ). All the nodes know the value of Δ. The time is divided into uniform intervals of 4 ms, and the TESLA key disclosure delay 'd' is 3 time intervals. The network links are bi-directional and dynamic.

LEACH Protocol

LEACH (Low Energy Adaptive Clustering Hierarchy) is a hierarchical-based routing protocol which uses random rotation of the nodes to be the cluster-heads to evenly distribute energy consumption in the network. Sensor network protocols are quite simple and hence are very susceptible to attacks like Sinkhole attack, Selective forwarding, Sybil attack, Wormholes, HELLO flood attack, Acknowledgement spoofing, altering and replaying routing information. For example, Selective forwarding and HELLO flood attack affects networks which use clustering based protocols like LEACH.

The authors (Heinzelman et al., 2000) introduced a hierarchical clustering algorithm for sensor networks, called Low Energy Adaptive Clustering Hierarchy (LEACH). LEACH arranges the nodes in the network into small clusters and chooses one of them as the cluster-head. Node first senses its target and then sends the relevant information to its cluster-head. Then the cluster head aggregates and compresses the information received from all the nodes and sends it to the base station. Low Energy Adaptive Clustering Hierarchy (LEACH) is the first hierarchical cluster-based routing protocol for wireless sensor network which partitions the nodes requiring the data using CDMA (Code division multiple access). This protocol is divided into rounds; each round consists of set up phase and steady phase.

Set-up Phase

Any node can become a CH randomly (Heinzelman et al., 2000). This decision is dependent on when the node was CH previously. The node that was not elected as CH for long time has more probability of being elected as CH than the recently elected nodes. This is calculated by threshold value, T (n). The threshold value depends upon the desired percentage p to become a cluster head, the current round r, and the set of nodes that have not become the cluster head in the last 1/p rounds, denoted as G. with the received messages in the cluster, CH creates a TDMA schedule, picks a CSMA code randomly and broadcasts the TDMA table to cluster members. Any node wanting to be the CH, selects a value, between 0 and 1 calling willing. If willing is less than the threshold value, T (n), then the node becomes the cluster- head for the current round. Then each elected CH broadcasts an advertisement message to the remaining nodes in the network to join their clusters. Based on the signal strength of the advertisement message, the non-cluster head nodes opt to join the clusters. In the set-up phase, the cluster head nodes are independently selected from all the sensor nodes and several clusters are constructed dynamically.

Steady Phase

At the starting of each round based on current energy level every node advertises it probability to be the CH to all the other nodes. Depending upon the received signal strength of each non CH, CH for this round is selected. In LEACH protocol, time is divided into many rounds. In each round, every node is suitable to be CH according to a predefined condition. In the steady phase called data transmission phase, member nodes in every cluster send data to their CH. The CH aggregates the data received from member nodes and sends the aggregated data to the BS.

Related Work

The authors (Haosong Gou et al., 2010) proposed an improved LEACH (LEACH-C) algorithm called partition-based LEACH (pLEACH), which partitions the network into optimal number of sectors, and then selects the node with the highest energy as the head for each sector, using the centralized calculations. The authors (Farooq et al., 2010) developed Multi-hop Routing with Low Energy Adaptive Clustering Hierarchy (MR-LEACH) protocol. In order to prolong the lifetime of WSN, MR-LEACH partitions the network into different layers of clusters. Cluster heads in each layer collaborates with the adjacent layers to transmit sensor's data to the base station. Ordinary sensor nodes join cluster heads based on the Received Signal Strength Indicator (RSSI). The BS controls the transmission by the nodes based on Time Division Multiple Access (TDMA) schedule for each cluster-head. BS selects the upper layers cluster heads to act as super cluster heads for lower layer cluster heads. Thus, MR-LEACH follows multi-hop routing from cluster-heads to a base station to conserve energy. The authors (Wu Xinhua et al., 2010) evaluated the performance of LEACH and LEACH-C protocols. The evaluation showed that performances of these two routing protocols changed with the sink locations. Two novel concepts were proposed, i.e., Sensor Node Distribution Gravity and Distance Metric between sink and Gravity. The authors (Mu Tong et al., 2010) developed LEACH-B (LEACH-Balanced). Initially the cluster head is selected based on LEACH protocol. A second selection modifies the number of cluster heads based on node's residual energy. As a result, the number of cluster head is constant and near optimal per round. 2L-LEACH-M (Cunguang Zhang et al., 2010) supports node mobility. It divides the nodes into two levels: level 1 (cluster-head level) or level 0 (member level). This enables mobile nodes to find a cluster-head more easily and hence ensures higher success rate of data transfer between the cluster-head and collector-nodes even when nodes are moving.

The authors (Kumar et al., 2011) proposed I-LEACH (Improved LEACH) with two important changes. CH (Cluster Head) is selected based on residual energy instead of probability used in LEACH. Secondly coordinates are used in the formation of clusters such that CH is available close to every sensor node. LEACH-SM protocol, (Bakr et al., 2011) modifies the LEACH protocol by enhancing it with an efficient management of spares. One of the spare management features in LEACH-SM (Bakr et al., 2011) is to add the spare selection phase to LEACH. During this phase, each node decides in parallel whether it should become an active primary node, or a passive spare node. The spare nodes sleep. The authors (Deng et al., 2011) proposed a mobility-based clustering (MBC) protocol for wireless sensor networks with mobile nodes. In MBC, a sensor node elects itself as a cluster-head based on its residual energy and mobility. A non-cluster-head node aims at its link stability with a cluster head during clustering according to the estimated connection time. Each non-cluster-head node is allocated a timeslot for data transmission in ascending order in a time division multiple access (TDMA) schedule based on the estimated connection time. In the steady-state phase, a sensor node transmits its sensed data in its timeslot and broadcasts a join request message to join in a new cluster and avoids more packet loss when it has lost or is going to lose its connection with its cluster head.

The authors (Sharma.M et al., 2012) studied LEACH protocol, some of its modified versions and suggested a new version of LEACH called Energy Efficient Extended LEACH (EEE LEACH) protocol. The new version of LEACH protocol establishes multilevel clustering approach to minimize communication distance between nodes and introduces Master Cluster Heads along with Cluster Heads. The authors (Yektaparast et al., 2012) proposed an improvement on the LEACH Protocol by dividing, each cluster into 7 subsections called cells. Every cell has a cell-head. Cell-heads communicate with cluster-heads directly. They aggregate their cell information and therefore they prevent sensors from communicating. In addition, computation of the threshold value for a cluster-head selection formula is also modified. Ningbo Wang et al suggested a protocol called LEACH-R based on LEACH protocol. LEACH-R improved the selection of cluster-head and choose relaying node when compared to LEACH. Residual energy of the nodes is considered during selection of cluster-head. Low-energy nodes being selected as cluster-head was reduced. Based on both residual energy and distance to base station, relaying node is chosen from cluster-heads to become the relay node between the base station and the other cluster-heads. The authors (Mehta et al., 2012) improved the LEACH algorithm as Equalized Cluster LEACH(C-LEACH), which initializes and maintains uniform sized clusters uniformly across the network. C-LEACH also incorporates the concept of adoption where orphaned cluster nodes are efficiently incorporated into neighboring clusters. The revised cluster routing algorithm E-LEACH (Jia Xu et al., 2012), enhances the hierarchical routing protocol LEACH. In the E-LEACH algorithm, the residual power of the sensor nodes is used in balancing the network loads and the round time depending on the optimal cluster size. The authors (Tripathi et al., 2012) proposed a new cluster head selection method for LEACH clustering routing protocol. It balances the energy consumption of every sensor node in a sensor network.

FLEACH (Oliveria et al., 2007), secures node to node communication in LEACH-based network. It used random key pre-distribution scheme with symmetric key cryptography to enhance security in LEACH. SLEACH (Adrian et al., 2005), provides security in LEACH by using the building block of SPINS (Security Protocol for Sensor Network), symmetric-key methods and MAC (Message Authentication Code). SLEACH protects against selective forwarding, sinkhole and HELLO flooding attacks. It prevents intruder to send bogus sensor data to the CH and CH to forward bogus message. But SLEACH was unable to avoid crowd in the time slot schedule of a cluster, causing DOS attack or lowers the throughput of the CH and does not guarantee data confidentiality. The solution is meant to protect only outsider attack. The MS-LEACH (El Saadawy et al., 2012) enhances the security of S-LEACH by providing data confidentiality and node to cluster head (CH) authentication using pair wise keys shared between CHs and their cluster members.

Many variations of LEACH have been presented which improves the random head selection, minimizes the distance between cluster heads, uses residual energy in the head selection algorithm and improves the TDMA schedules. But few security solutions to LEACH are suggested that uses random key pre distribution schemes, SPIN blocks and protects only outsider attacks. So, in this work a secure LEACH is proposed using a light weight TESLA based certificate. The TESLA based certificates are used in securing MAODV (R.Shyamala et al., 2013) and Location based routing protocol, namely, geographic multicasting routing protocol (GMR) (Shyamala et al., 2012). The impact of routing attacks in GMR is also studied (Shyamala et al., 2009, 2011).

Node Membership Certificate

All the sensor nodes in the network have a certificate called the Node Membership Certificate. This certificate is issued by the trusted certificate authority (CA) which is the base station in WSN. The format of the Node Membership Certificate is given in Figure 1. Only nodes possessing the Node Membership Certificates can participate in the routing. The base station periodically distributes the Node Membership Certificate to all the sensor nodes in the network.

Node_ID	Node_Key	Life_Time	SIGN
3 Bytes	16 Bytes	2 Bytes	16 Bytes

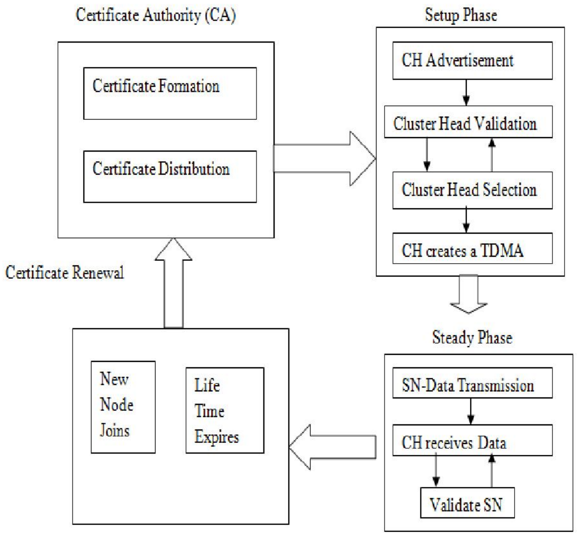
Figure 1. Node Membership Certificate

The TESLA (Mathias Bohge et al., 2003) based Node Membership Certificate is shown in Figure 1. Each certificate is based on the key generated at time interval ‘t’ using a one way hash function (F) as a TESLA key to calculate the SIGN, and to encrypt the Node_Key. The CA discloses the seed of the one way hash function after 3 time intervals, which is the disclosed delay time (d). In the Node Membership Certificate, the authentication key (AK) of each sensor node is calculated by the CA and is encrypted by the TESLA key of the CA and is represented as Node_Key. The signature is referred as SIGN, which is the Message Authentication Code (MAC). SIGN is calculated using the TESLA key of the CA. The node identity is represented by the Node_ID, and the expiry time of the certificate is represented as the Life_Time. The Node_ID occupies 3 bytes and Life_Time occupies 2 Bytes. The Node_Key and SIGN fields occupy 16 Bytes, since, it uses MD5 (128 bits) as a hash function to generate one way hash chain of TESLA.

Working of Secure LEACH

The Secure LEACH is implemented using TESLA based certificate. It also consists of the cluster formation and distribution algorithm, secure CH selection algorithm, secure data transfer algorithm and certificate renewal algorithm. The coordination of these algorithms is shown in Figure 2.

Initially, Certificate Authority (CA) constructs and distributes Node Membership Certificate to all the sensor nodes in the network. A Node with a Node Membership Certificate can only participate in secure cluster head selection. In the setup phase, the sensor nodes which want to become a cluster head broadcast its willingness using a random number between 0 to 1 as given in Step 6 of Secure Head Selection algorithm. The threshold value is calculated as in Heinzelman et al., 2000. The node’s whose random number is less than the threshold and having a valid Node Membership Certificate would be selected as the cluster head for the current round. N numbers of nodes are assumed in the network. The variable CH_Count denotes the number of cluster heads. LEACH ensures that all the nodes become cluster heads only once in (N/CH_Count) by confirming if the node has become a cluster head in the recent rounds (No_of_ rounds mod N/CH_Count) or not. After the cluster head selection, all the selected cluster heads send an advertisement message to the remaining sensor nodes in the network. Based on the received signal strength of the advertisement message, the remaining sensor nodes decide their cluster heads for the current round and send back a join request message with the Node Membership certificate to their selected cluster heads informing their membership which leads to cluster formation. For avoiding collision in the network LEACH uses TDMA schedule. According to the number of nodes in each cluster, the cluster head validates the members and creates a TDMA schedule and broadcasts it to its member nodes.



SN - Sensor node CH – Cluster head

Figure 2. Design of Secure LEACH

The Next Phase is the steady state phase which is the data transmission step. During this phase, nodes in each cluster send their data along with the Node Membership Certificate based on the allocated transmission time to their local cluster heads. To reduce the energy dissipation, the receiver of all non-cluster head nodes would be turned off until the nodes defined allocated time. After receiving all the data from the nodes, the cluster head validates the Node by Node_Key and aggregates all the data sent from the members into a single signal and transfers it to the base station by appending its Node Membership Certificate.

```
Class Node Membership Certificate {
Private:
int* Node_ID;
Char *Node_Key;
int *Life_Time;
Char * SIGN;
};
```

ALGORITHM: *Secure_Head Selection Algorithm Takes A Set Of N Sensor Nodes And Selects Cluster Heads In Successive Iterations.*

```
1.  [Initialize]
    No_of _rounds =0;
    while TRUE
    do
        if Network_Energy<= 0
        then
            return;
        else
2.  [Check the available number of sensor nodes]
    for i = 1 to N
    do
        if (Node[i] → Energy > 0)
        then
            NodeCount++;
        end if;
    end for;
3.  [Secure Cluster-head Selection]
    for i = 1 to N
    do
        if (Node[i] → Energy >0 ) &&
            (IsValid(Node[i])
        then
            Willing = random();
            if (Willing < Threshold
            (No_of_rounds, CH_Count))
            then
                Node[i] → type ='CH';
                CH_Count++;
                Send an Advertisement to
                remaining Sensor Node(SN);
            end if;
        end if;
    end for;
4.  [Attach SN to the Cluster]
    for i = 1 to N
    do
        if ( (Node[i] → Energy >0 )&&
            (IsValid(Node[i]) &&
            (Node[i] → type ='SN') )
        then
            attach SN to the Cluster;
            calculate TDMA-SN;
        end if;
    end for;
5.  [Increment the number of iterations]
    if CH_count> 0
    then
        No_of _rounds++;
    end if;
    end while;
6.  end.
```

ALGORITHM: Threshold (No_of_rounds, CH_Count) *Calculates threshold value based on desired percentage (P) to become CH, the Current round (No_of_round) and the set of nodes that have not been selected as CH in the previous rounds.*

```
1.  for i=1 to CH_Count
    do
    $TV = P[i]/(1- (p[i] (No\_of\_rounds) \bmod (p^{-1})))$
    end for;
2.  return TV;
```

Algorithm: IS_VALID (Node[i]) gets the seed of key chain (S_0) at time t, and the certificate of any node Node[i]. This algorithm verifies the certificate of Node[i].

```
1. [ Initialize]
   Get SIGN from CERT(Node[i]);
2. [Calculate the TESLA Key of CA]
   From $S_0$, calculate the TESLA key using MD5.
   New_Sign(Node[i]) = Using the TESLA key,
   calculate MAC of Node Membership Certificate.
3. if (SIGN(Node[i]) = = New_Sign(Node[i]) )
   then
       Decrypt Node_Key;
       Node[i].key =Node_Key;
       return 1;
   else
       return 0;
```

ALGORITHM: ***Secure_Data Transfer Algorithm*** *CH Validates and aggregates a set of N data and securely forwards it to the base station.*

```
1.  [Initialize ]
    No_of _rounds =0;
2.  while TDMA
    do
    [Secure Data Transmission]
        for i = 1 to N
        do
            if (TimeSlot(Node[i]) &&
                IsValid(Node[i]))
            then
            CH→ Node[i] → data = Node[i] → data
            end if;
        end for;
        Aggregate Data( );
        Append Data || Node Membership
        Certificate of CH
3.      if CH_Count> 0
        then
        No_of _rounds++;
        end if;
    end while;
```

4. **Stop**

3. Results

Performance Analysis

To evaluate the effectiveness of the proposed algorithm, the secure LEACH is simulated using NS-2 (NS-2: http://www.isi.edu/nsnam/ns/). The goal of the evaluation is to test the effectiveness of the secure LEACH variations under normal conditions.

The size of the data payload is 512 bytes. This simulation is based on a sensor network with 100 sensor nodes uniformly distributed in the dimension of 100m X 100m (Tian et al, 2012). Node 1 is the base station. Table 1 is the simulation parameters used. The size of the cluster was varied as 5,10,15,20 and 25 and the results are compared with unsecure LEACH with routing attacks. The network performance is evaluated, using the packet delivery ratio (PDR), Network Throughput (Nth), Average Delay (AD) and Energy consumption (EC) metrics.

Packet Delivery Ratio (PDR)

The packet delivery ratio (PDR) is defined as the ratio of the total number of data packets received by the destination node to the number of data packets sent by the source node as given by equation (1). Figure 3 shows the PDR of secure LEACH by varying the cluster size. From Figure 3 PDR is 62.06% for the cluster size of 5 nodes at 50 ms of simulation. At 150 ms the PDR reaches the value of 64.32% with the cluster size of 5 and 67.2% for the cluster size of 25. At 250 ms the PDR is 71.52% for the cluster with 25 nodes. These values are listed in the column 3 of the Table 2. From these values it is observed that when the cluster size increases the performance of secure LEACH is high and the PDR of secure LEACH varies from 58.9% to 71.52% for varying cluster sizes and hence, the secure LEACH attains a good mean PDR of 66.15% at cluster size of 25 nodes.

In Figure 4, PDR of secure LEACH is compared with unsecure LEACH with routing attacks such as Sybil, wormhole, rushing and black hole. From the Figure 4, the unsecure LEACH with Sybil attack has the PDR of 52.51% at 100ms. Wormhole has the value of PDR 51.16% at 200 ms, black hole attack has the PDR of 44.12 % at 50 ms, and rushing attack has the PDR of 44.66% at 50 ms. The black hole attack has the lowest PDR of 44.12% and causes more damages when the routing attacks are introduced in secure LEACH a mean PDR of 59.38% for cluster size 10 is achieved and the values are listed in Table 3 of column 3. Hence the routing attacks were restricted and therefore, PDR is improved by secure LEACH.

Table 1. Simulation Parameters

Examined Protocol LEACH Simulator NS-2 Simulation time 250 Sec Simulation area 100x100m Number of sensor nodes 100 Number of base stations 1 Number of malicious nodes 1-10	Transmission range 250m Movement model Static Initial energy 5J RxPower 1.75mW TxPowe r 1.75mW SensePower 1.75mW IdlePower 1.75μW

$$\text{Packet Delivery Ratio (PDR)} = \frac{\sum \text{of packets received by the destination node}}{\sum \text{of packets sent by the source node}} \quad (1)$$

$$\text{Network Throughput (NTh)} = \frac{\text{packets size}}{\text{Transmission Time}} \quad (2)$$

Table 2. Performance of Secure LEACH with varying cluster size 5,10,15,20 and 25.

Cluster Size	Time	PDR in %	NTh in (Mbps)	Energy Consumption in Joules	Average Delay in Joules
5	50	62.06	333.33	144.12	21.0341
	100	62.02	308.51	192.74	23.7456
	150	64.32	284	245.77	26.1107
	200	60.50	271.15	302.86	29.306
	250	61.99	264.15	322.62	30.9055
	Mean	**62.178**	**292.228**	**241.622**	**26.2204**
10	50	58.90	355.11	163.23	23.0024
	100	61.69	337.44	201.98	26.4563
	150	61.97	315	276.55	29.8004
	200	59.57	300.96	300.64	31.7031
	250	58.19	293.96.	311.76	33.0754
	Mean	**60.064**	**327.1275**	**250.832**	**28.8075**
15	50	63.03	355.55	169.44	25.8012
	100	60.51	340	210.78	26.7751
	150	60.97	317.6	264.83	28.6093
	200	62.76	302.88	297.19	31.443
	250	63.23	296.22	313.86	33.1954
	Mean	**62.1**	**322.45**	**251.22**	**29.1648**
20	50	62.60	366.22	181.76	27.1752
	100	61.20	347.87	191.77	29.4571
	150	65.61	325.2	216.54	34.9037
	200	65.13	311.15	275.63	33.7463
	250	61.27	303.58	314.47	36.6512
	Mean	**63.162**	**330.804**	**236.034**	**32.3867**
25	50	61.42	372.88	197.41	32.0423
	100	63.88	354.04	216.73	36.9824
	150	67.20	331.8	252.52	37.4952
	200	66.73	316.34	336.96	39.115
	250	71.52	309.24	352.87	42.5863
	Mean	**66.15**	**336.86**	**271.298**	**37.6442**

Network Throughput (Nth)

The network throughput (NTh) is calculated using equation (2). Figure 5 is the network throughput of secure LEACH, when the cluster size is varied from 5 to 25 nodes. From Figure 5, at 50 ms the network throughput is 333.33, 355.11, 355.55, 366.22 and 372.88 Mbps for the cluster size of 5,10,15,20, and 25 respectively. At 100 ms the network throughput is 340 Mbps for the cluster with 15 nodes. But at the same simulation time, cluster with 25 nodes achieves 354.04 Mbps. The value of network throughput at 150 ms of simulation varies from 284 to 331.8 Mbps for varying cluster sizes. The network throughput of 309.24 Mbps is reached at 250 ms for the cluster with 25 nodes. From Table 2 the mean network throughput is 336.86 Mbps for the cluster with 25 nodes which shows that secure LEACH, validates the data packets with optimal network throughput.

Figure 6, is the network throughput comparison of secure and unsecure LEACH with routing attacks. The mean throughput achieved in the presence of Sybil attack is 222.776 Mbps, 236.072 Mbps in case of wormhole attack, 228.352 Mbps in the presence of black hole attack and 231.370 Mbps in the presence of rushing attack and therefore Sybil affects the routing procedure of LEACH resulting in network throughput of 222.776 Mbps. These routing attacks are limited in the secure LEACH with the mean network throughput of 300.782 Mbps as listed in the Table 3.

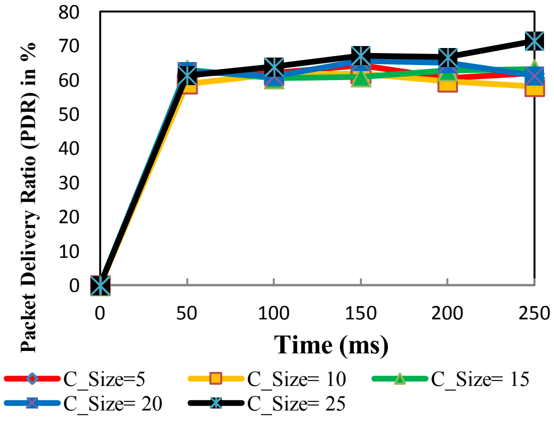


Figure 3. Packet Delivery Ratio of Secure LEACH by varying Cluster Size (C_Size) from 5 to 25.

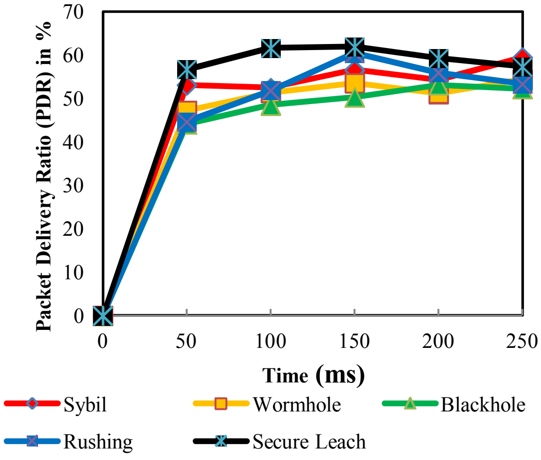


Figure 4. Comparison of Packet Delivery Ratio of Secure LEACH and Unsecure LEACH in the presence of routing attacks.

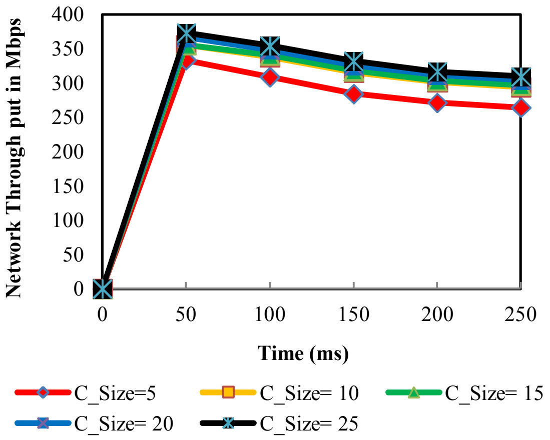


Figure 5. Network Throughput of Secure LEACH by varying Cluster Size (C_Size) from 5 to 25.

Table 3. Performance of Secure and Unsecure Leach with routing attacks of cluster size 10.

Routing attacks	**Time**	**PDR in %**	**NTh in Mbps**	**Energy Consumption in Joules**	**Average Delay in ms.**
Sybil Attack in unsecure LEACH	50	53.13	255.55	186.26	28.413
	100	52.51	236.17	199.73	31.741
	150	56.61	216.00	216.46	36.267
	200	54.25	207.30	253.74	37.787
	250	59.54	198.86	227.11	36.194
	Mean	**55.2**	**222.77**	**216.66**	**34.084**
Wormhole Attack in unsecure LEACH	50	47.25	261.11	180.08	23.124
	100	51.37	248.51	192.17	21.965
	150	53.61	231.8	216.54	22.364
	200	51.16	222.34	216.92	23.668
	250	54.41	216.6	200.63	23.004
	Mean	**51.56**	**236.07**	**201.27**	**22.825**
Black hole Attack in unsecured LEACH	50	44.12	252.22	190.89	26.023
	100	48.49	239.78	205.45	26.474
	150	50.32	224.40	220.45	26.337
	200	53.19	214.80	260.25	28.896
	250	52.26	210.56	255.23	29.69
	Mean	**49.68**	**228.35**	**226.45**	**27.48**
Rushing Attack in unsecured LEACH	50	44.66	254.44	182.52	23.524
	100	51.84	242.97	195.36	22.514
	150	60.47	227.8	198.47	21.568
	200	55.97	218.26	206.87	21.487
	250	53.38	213.39	214.52	21.158
	Mean	**53.26**	**231.37**	**199.548**	**22.05**
Secured LEACH with routing attack	50	56.72	331.11	163.23	22.0345
	100	61.68	316.17	170.15	23.8968
	150	61.91	296.00	189.56	26.5145
	200	59.29	283.65	198.75	29.8731
	250	57.34	276.98	211.06	32.9602
	Mean	**59.38**	**300.78**	**186.55**	**27.0558**

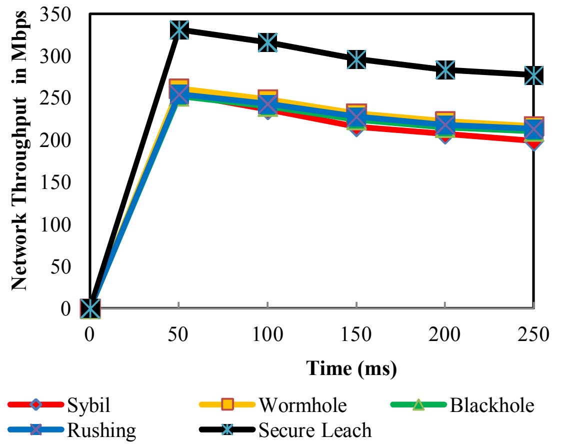


Figure 6. Comparison of Network Throughput of Secure LEACH and Unsecure LEACH with routing attacks of cluster size 10.

Energy Consumption (EC)

Figure 7, shows the total network energy consumption of secure LEACH when the cluster size is varied from 5 to 25 nodes. The energy consumption by the cluster of 25 nodes is 352.87 joules at 250 ms. If the cluster size is 5 nodes, then, the total network energy at 250 ms is at most 322.62 joules. These values are listed in column 5 of Table 2. When the cluster size is 25 nodes, many nodes require node verification and therefore require more energy.

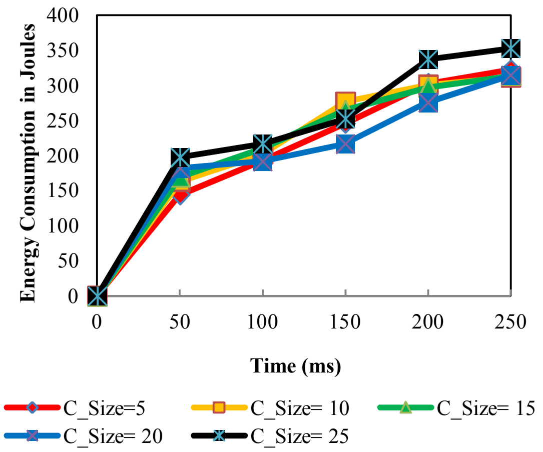


Figure 7. Energy Consumption of Secure LEACH by varying Cluster Size (C_Size) from 5 to 25.

Figure 8, is the energy consumption of secure LEACH and unsecure LEACH with routing attacks. In unsecure LEACH black hole attack consumes 255.23 joules at 250 ms which is very high compared to other routing attacks. The secure leach with routing attacks consumes total of 211.06 joules by restricting all the routing attacks as in Table 3.

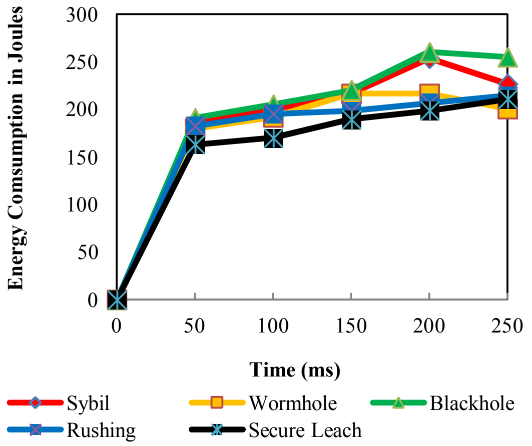


Figure 8. Comparison of Energy Consumption of Secure LEACH and Unsecure LEACH with routing attacks of cluster size 10.

Average Delay (AD)

Figure 9, is the average network delay of secure LEACH by varying the cluster size. From Figure 9, the cluster size with 5 nodes, has the average delay of 21.0341 ms at 50 ms of simulation. When the time increases from 50 ms to 100 ms the delay varies from 21.0341 ms to 23.7456 ms. At 150 ms the average delay of the network reaches the value of 26.1107 ms for the cluster size of 5 nodes and 37.4952 ms for the cluster size of 25 nodes. At 250 ms the delay is higher with 42 ms for the cluster size of 25 nodes. These values are listed in column 6 of Table 2. From these values it is observed that when the cluster size increases the performance of secure LEACH is high and the delay of secure LEACH varies from 21.0341 ms to 42.5863 ms for varying cluster sizes and hence, secure LEACH attains a good average delay of 26.224 ms at cluster size of 5 nodes.

In Figure 10, average delay of secure LEACH is compared with unsecure LEACH with Sybil, wormhole, rushing and black hole active attacks. From Figure 10, unsecure LEACH with Sybil attack has a delay of 31.741 ms at 100 ms of simulation. The wormhole has a delay of 23.668 ms at 200 ms, black hole has a delay of 29.69 ms at 250 ms and, rushing attack has a delay of 23.524 ms at 50 ms. The rushing attack has the lowest delay of 21.158 ms. Sybil attack has a mean delay of 34.084 ms which causes more damage to routing. The above routing attacks are introduced in secure LEACH and give a constant mean delay of 27.05582 ms with cluster size of 10 nodes and hence the routing attacks are restricted and delay is slightly more because of TESLA based certificates. Because they are verified by disclosing the TESLA key which requires more waiting time.

4. Discussion

In this work, TESLA-based certificate is used to secure the LEACH for low power Wireless sensor networks. TESLA based certificates reduces the energy consumption in the presence and absence of attacks and it resists the routing attacks. Hence, TESLA based certificates resists the attacks in LEACH and enhances the performance of WSN. A cluster-based multicast of larger size will improve the performance. The simulation study shows that the TESLA-based Certificate for Routing Protocol is possible in wireless sensor networks. Further, the delay of secure LEACH is more and if it is reduced the performance will improve greatly. So, instead of TESLA based certificate which has the disclosure delay replaced by other broadcast authentication functions such as BiBa, HORSE. The tradeoff between energy and delay is a critical issue for further study.

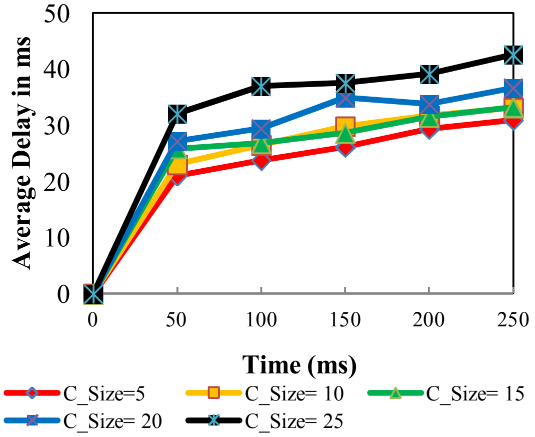


Figure 9 Average Delay of Secure LEACH by varying Cluster Size (C_Size) from 5 to 25.

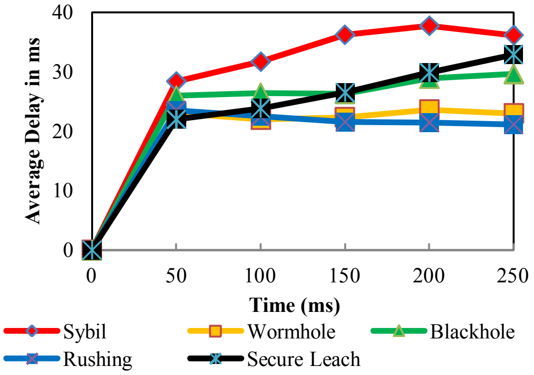


Figure 10 Comparison of Average Delay of Secure and unsecure LEACH with routing attacks of cluster size 10.

References

1. A. C. Ferreira, M. A. Vilaca, L. B. Oliveira, E. Habib, H. C. Wong, and A. A. F. Loureiro. On the security of cluster-based communication protocols for wireless sensor networks. In 4th IEEE International Conference on Networking (ICN'05), 2005; 3420: 449-458.
2. Akyildiz W.S., Sankarasubramaniam Y. and Cayirci E. A Survey on Sensor Networks. IEEE Communications Magazine. 2002; 40, 102-116.
3. Bakr, B.A. and Lilien, L. Extending Wireless Sensor Network Lifetime in the LEACH-SM Protocol by Spare Selection. In the IEEE Proc. of Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS). 2011; 277 – 282.
4. Cunguang Zhang, Jianming Liu, Hongzhou Li and Xiaohong Jiang. Two-level routing protocol for mobile sensor network based on LEACH algorithm. In the IEEE Proc. of Intelligent Computing and Integrated Systems (ICISS). 2010; 950 – 953.
5. Deng, S. and Li, J.; Shen, L. Mobility-based clustering protocol for wireless sensor networks with mobile nodes. IEEE Journal on Wireless Sensor Systems, IET. 2011; l1(1): 39 – 47.
6. El Saadawy, M. and Shaaban, E. Enhancing S-LEACH security for wireless sensor networks. In the IEEE Proc. of Electro/Information Technology (EIT) . 2012; 1-6.
7. Farooq M.O., Dogar A.B. and Shah G.A. MR-LEACH: Multi-hop Routing with Low Energy Adaptive Clustering Hierarchy. In the IEEE Proc. of Sensor Technologies and Applications (SENSORCOMM). 2010; 262 – 268.
8. Haosong Gou and YounghwanYoo. An Energy Balancing LEACH Algorithm for Wireless Sensor Networks. In the IEEE Proc. of Information Technology: New Generations (ITNG). 2010; 822 – 827.
9. JiaXu; Ning Jin, Xizhong Lou, Ting Peng, Qian Zhou and Yanmin Chen. Improvement of LEACH protocol for WSN. In the IEEE Proc. of Fuzzy Systems and Knowledge Discovery (FSKD). 2012; 2174 – 2177.
10. Kumar, N. and Kaur, J. Improved LEACH Protocol for Wireless Sensor Networks. In the IEEE Proc. of Wireless Communications, Networking and Mobile Computing (WiCOM), 2011; 1 – 5.
11. L. B. Oliveira, H. C. Wong, R. Dahab, and A. A. F. Loureiro. On the design of secure protocols for hierarchical sensor networks. International Journal of Networks and Security, 2007; 2(3/4):216–227.
12. Mathias Bohge and Wade Trappe. An Authentication Framework for Hierarchical Ad Hoc Sensor Networks. In Proc. 2nd ACM Workshop on Wireless Security. 2003; 79 – 87.

13. Mehta, R., Pandey, A. and Kapadia, P. Reforming clusters using C-LEACH in Wireless Sensor Networks. In the IEEE Proc. of Computer Communication and Informatics (ICCCI). 2012; 1 – 4.
14. Mu Tong and Minghao Tang. LEACH-B: An Improved LEACH Protocol for Wireless Sensor Network. In the IEEE Proc. of Wireless Communications Networking and Mobile Computing (WiCOM). 2010; 1-4 .
15. NS-2: http://www.isi.edu/nsnam/ns/.
16. R.Shyamala and S.Valli. Impact of Blackhole and Rushing Attack on the Location-Based Routing Protocol for Wireless Sensor Networks. Proceedings of Advances in intelligent system and computing. 2012; 176: 349-359.
17. Sharma M. and Sharma K. An Energy Efficient Extended LEACH (EEE LEACH). In the IEEE Proc. of Communication Systems and Network Technologies (CSNT), 2012; 377-382.
18. Shyamala R and Valli S. Secure route discovery in MAODV for Wireless Sensor Networks. UbiCC Journal, 2009; 4: 775-783.
19. Shyamala Ramachandran and Valli Shanmugam. Securing GMR Protocol using TESLA Based Certificate for WSN. European Journal of Scientific and Research. 2013; 94(2): 186-196.
20. Shyamala Ramachandran and Valli Shanmugam. Impact of Sybil and Wormhole Attacks in Location Based Geographic Multicast Routing Protocol for Wireless Sensor Networks. Journal of Computer Science. 2011; 7:973-979.
21. Shyamala Ramachandran and Valli Shanmugam. Performance Comparison of Routing Attacks in MANET and WSN. International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), 2012; 3: 41-52.
22. Tripathi R.K., Singh Y.N. and Verma, N.K. N-LEACH, a balanced cost cluster-heads selection algorithm for Wireless Sensor Network. In the IEEE Proc. of Communications (NCC). 2012; 1-5.
23. W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan. Energy-efficient communication protocol for wireless micro sensor networks. In Proceedings of the 33rd Annual Hawaii International Conference on system Sciences. 2000; 2: 3005-3014.
24. Wu Xinhua and Wang Sheng, Performance Comparison of LEACH and LEACH-C Protocols by NS-2. In the IEEE Proc. of Distributed Computing and Applications to Business Engineering and Science (DCABES). 2010; 254 – 258.
25. Yektaparast, A. Nabavi, F H and Sarmast, A. An improvement on LEACH protocol (Cell-LEACH). In the IEEE Proc. of Advanced Communication Technology (ICACT). 2012; 992 – 996.

4/2/2013