```
do
  if newCH = CH
      then B.S. ← currentCH[MAC[KN-BS,M]]                4 bytes
          Ni ← B.S.[ MAC[KN-BS,M, [KN-N]]]               4 bytes
while [current round ≠ end]
```

At the beginning of a new round, the cluster head sends a verification message (verification [M]) with key (KN-N) to neighbour's nodes. After receiving the message, nodes reply to the cluster head's request by a verification message encrypted by the shared key ([KN-N, authentication [M]]) requesting to join the cluster. However, the cluster head needs to make sure that it doesn't allow the number of nodes to exceed the allowed number in cluster (Ni<_ 20 Ni). On the other hand, nodes must request to join the clusters closer to them to reduce the energy consumption in receiving and transmitting (new CH > signal new CH).

```
while [current round ≠ end]
    then Ni ← newCH[MAC[KN-N, M]]                         4 bytes
    while newCH ← Ni ≤ 20 Ni
      and newCH > signal newCH ← Ni
        then newCH ← Ni[MAC[KN-N, M]]                     4 bytes
```

4.3 Transmission

The network nodes have three stases; sensing, listening/transmitting and sleeping. Sensing takes place when the nodes are sensing the environment. Listening/Transmitting happens when nodes are expecting to have communication with the cluster head or base station. Sleeping takes place when the nodes are node in sensing or listening/Transmitting modes. This requires the nodes to be in sleep mode to avoid the overhearing which consume nodes energy.

```
while [current round ≠ end]
   then if Ni ≠ sensing data or CH ← Ni ≠ sending data
          do sleep ← CHStatus
             sleep ← NiStatus
      else
          Listen ← CHStatus
          Listen ← NiStatus
          CH ← Ni[MAC[KN-N, M]]                           4 bytes
```

Nodes are required to have a log for the connections attempts that are initialled with them. When the attempts reach a predefined threshold, a flag is raised to the cluster head and the base station. The base station has to perform the necessary actions in case the sensor is under attack.

```
while [current round ≠ end]
    then while Ni = sleep or CH = sleep
          if(CH ← newCH[MAC[KN-N, [M]])
            CH ← report
          if(CH ← Ni[MAC[KN-N, M]])
            B.S ← report
```

5. Simulation

The implementation software of LS-LEACH was carried using network simulator NS-2. NS-2.34 version was used in this implementation and simulation. NS2 is open source software under GPL (general public license). Moreover, NS2 is built in C++ and the interface is in OTcl language which is an object oriented extension of TCL language. Further, the operating system environment of the simulation was Linux Ubuntu 10.04 LTS installed on system with 2.5 GHz Intel Core 2 Duo and 4 GB memory.

The implementation of LS-LEACH was executed by adding new parameters and functions to the existing LEACH in NS2. Most of the changes were done in the source files of LEACH which are located in the ns-2.34 (as in version 2.34) directory in folder 'mit'. Other changes were also done in different files for the purpose of the linking of the TCL and C++ as TCL language is used as the interface for NS2 and OTcl is liking between TCL and C++.

5.1 Simulation Parameters

In simulating LS-LEACH, we have used the following parameters shown in Table 1.

Table 1: Simulation Parameters

TABLE I. SIMULATION PARAMETERS

Parameter	Value
NS-2 Version	2.34
MAC Protocol	Sensors
Channel Type	WirelessChannel
Propagation	TwoRayGround
Queue	DropTail
Queue Length	100
Antenna	OmniAntenna
Area	1000 x 1000
Routing Protocol	LEACH
Number of Nodes	100
Number of Cluster	5
Nodes in Cluster	20
Simulation Time	3600 sec or CH < 5
Node Initial Energy	2j
Equal Energy (Start Up)	YES
CSThresh	1 nW
RXThresh	6 nW
Round Period	Each 20 sec

6. Simulation Results

The performance of the system was measured using the system throughput, network life time and the total energy consumption.

6.1. System throughput

Fig. 3 shows the system throughput comparing between the classical LEACH protocol, and the proposed LS-LEACH. The proposed protocol has better performance because it tries to mitigate the ideal listening by putting the nodes in sleeping

state which reduce the power consumption allowing the nodes to live longer and to reduce the collisions. The normal Leach protocol stopped performing because all the nodes died at time 360 which is after 19 rounds. However, the proposed protocol kept performing until time 475 which is after 24 rounds.

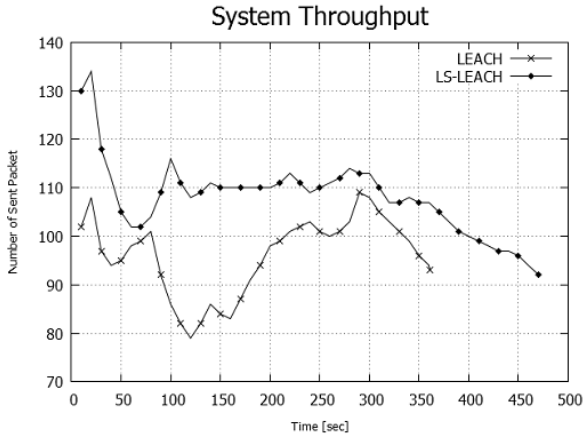

Fig. 3. System Throughput
Figure 3: System Throughput

6.2. Network Life Time

Fig. 4 shows the comparison between the normal LEACH protocol and the proposed protocol in terms of network life time. At time 210 sec, normal LEACH protocol started to lose nodes, and by time 368, most nodes run out of power (when CH < 5).

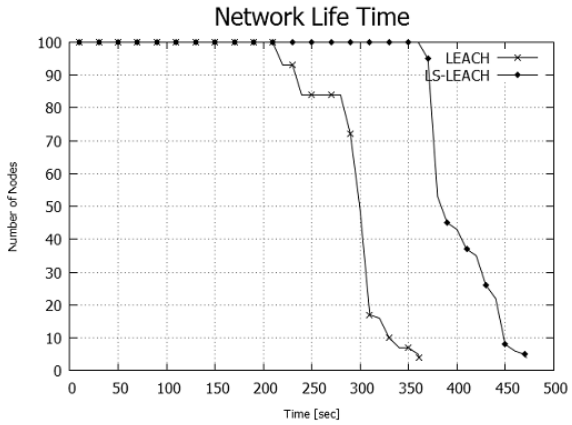

Fig. 4. Network Life Time
Figure 4: Network Life Time

On the other hand, LEACH with security lost the first node at time 360 and lost most of the nodes (when CH <5) at time 471.

6.3. Energy Consumption

Comparing the energy consumption between normal LEACH and leach with security in Fig. 5, we find the proposed protocol has less power consumption. As a result, normal LEACH lasted until time 364 and the proposed protocol lasted until time 371. The increase of power consumption in LEACH protocol started at time 210 with the loss of the first node. As a result, the other nodes faced more load due to the increase of power consumption which reduced the network life. On the other hand, the proposed protocol lost the first node at time 360. This reduced the power consumption and increased the network life time.

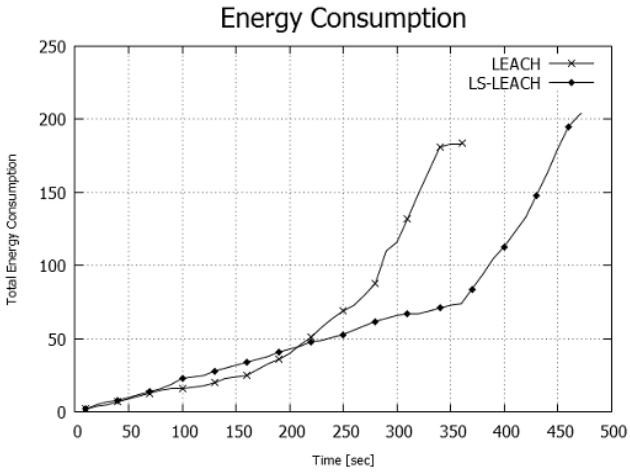

Fig. 5. Total Energy Consumption
Figure 5: Total Energy Consumption

7. Conclusions

In this paper we have introduced and implemented LS-LEACH which is an improvement of LEACH protocol. After improving LEACH protocol power consumption and adding the security measures, the protocol performed better in terms of the system throughput, network life time and the total energy consumption. The proposed protocol provided a secure authentication protocol for the network where the new nodes requesting to join the network must be authenticated in order to join the network.

References

[1] M. V. Ramesh, A. B. Raj, and T. Hemalatha, "Wireless Sensor Network Security: Real-Time Detection and Prevention of Attacks," in Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on, Mathura, 2012, pp. 783-787.

[2] L. Gheorghe, R. Rughinis, R. Deaconescu, and N. Tapus, "Authentication and Anti-replay Security Protocol for Wireless Sensor Networks," in Systems and Networks Communications (ICSNC), 2010 Fifth International Conference on, Nice, France, 2010, pp. 7-13.

[3] M. Rahman, S. Sampalli, and S. Hussain, "A robust pair-wise and group key management protocol for wireless sensor network," in GLOBECOM Workshops (GC Wkshps), 2010 IEEE, Miami, FL, 2010, pp. 1528-1532.

[4] M. El-Saadawy and E. Shaaban, "Enhancing S-LEACH security for wireless sensor networks," in Electro/Information Technology (EIT), 2012 IEEE International Conference on, 2012, pp. 1-6.

[5] H. Soroush, M. Salajegheh, and T. Dimitriou, "Providing transparent security services to sensor networks," in Communications, 2007. ICC'07. IEEE International Conference on, Glasgow, 2007, pp. 3431-3436.

[6] D. Martynov, J. Roman, S. Vaidya, and H. Fu, "Design and implementation of an intrusion detection system for wireless sensor networks," in Electro/Information

Technology, 2007 IEEE International Conference on, Chicago, IL, 2007, pp. 507-512.
[7] L. Sang Hyuk, L. Soobin, S. Heecheol, and L. Hwang-Soo, "Wireless sensor network design for tactical military applications : Remote large-scale environments," in Military Communications Conference, 2009. MILCOM 2009. IEEE, 2009, pp. 1-7.
[8] H. Modares, R. Salleh, and A. Moravejosharieh, "Overview of Security Issues in Wireless Sensor Networks," in Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on, 2011, pp. 308-311.
[9] D. E. Burgner and L. A. Wahsheh, "Security of Wireless Sensor Networks," in Information Technology: New Generations (ITNG), 2011 Eighth International Conference on, 2011, pp. 315-320.
[10] A. Blilat, A. Bouayad, N. El Houda Chaoui, and M. E. Ghazi, "Wireless sensor network: Security challenges," in Network Security and Systems (JNS2), 2012 National Days of, 2012, pp. 68-72.
[11] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in International Conference on System Sciences, Maui, Hawaii, 2000, pp. 1-10.
[12] M. Guechari, L. Mokdad, and S. Tan, "Dynamic solution for detecting denial of service attacks in wireless sensor networks," in IEEE ICC Ad-hoc and Sensor Networking Symposium, Ottawa, ON, Canada, 2012, pp. 173-177.
[13] L. Bai and L. Batten, "Using Mobile Agents to Detect Node Compromise in Path-Based DoS Attacks on Wireless Sensor Networks," in Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on, Shanghai, China, 2007, pp. 2507-2510.
[14] Y. Xin, B. Tian, Q. Li, J.-y. Zhang, Z.-M. Hu, and Y. Xin, "A Novel Framework of Defense System Against DoS Attacks in Wireless Sensor Networks," in Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on, Wuhan, 2011, pp. 1-5.
[15] E. Stavrou and A. Pitsillides, "Vulnerability assessment of intrusion recovery countermeasures in wireless sensor networks," in Computers and Communications (ISCC), 2011 IEEE Symposium on, Kerkyra, 2011, pp. 706-712.
[16] V. Cionca, T. Newe, and V. Dadarlat, "On the (im) possibility of denial of service attacks exploiting authentication overhead in WSNs," in Sensors Applications Symposium, 2009. SAS 2009. IEEE, 2009, pp. 74-79.
[17] J. Xu, N. Jin, X. Lou, T. Peng, Q. Zhou, and Y. Chen, "Improvement of LEACH protocol for WSN," in Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on, 2012, pp. 2174-2177.
[18] Y. Wei, J. Heidemann, and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks," IEEE/ACM Transactions on Networking, vol. 12, pp. 493-506, 2004.
[19] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," Wireless networks, vol. 8, pp. 521-534, 2002.
[20] L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab, and A. A. Loureiro, "SecLEACH-A random key distribution solution for securing clustered sensor networks," in Network Computing and Applications, 2006. NCA 2006. Fifth IEEE International Symposium on, 2006, pp. 145-154.

Author Profile

Penumolu Ratnakumari Obtained the B.Tech degree in Information Technology(IT) from Vignan Engineering College,Vadlamudi. At present persuing the M.Tech in Computer Science and Engineering(CSE) Department at Guntur Engineering College , Guntur.

M. Koteswara Rao obtained the MCA from RVR&JC College of Engineering and M. Tech (CSE) from Nalanda Institute of Engineering & Technology, JNTU Kakinada. He has 6 years of teaching experience and working in Computer Science and Engineering (CSE) Department at Guntur Engineering College, Guntur.