ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 9, September 2014 Page No. 8389-8393

Comparative Analysis of Secure and Energy Efficient routing protocols in Wireless sensor network

Amanpreet Kaur[1], Dr. Sandeep Singh Kang[2]

[1]M.Tech Scholar, Department of Computer Science and Engineering,
Chandigarh Group of Colleges,Landran,Mohali,
preetaman6689@gmail.com

[2]HOD, Department of Computer Science and Engineering,
Chandigarh Group of Colleges,Landran,Mohali,
Sskang4u1@rediffmail.com

Abstract:*Hierarchical routing architecture divides the whole network into a group of cluster and only cluster head is responsible to forwarding the data to base station directly. In hierarchical based architecture of routing, the cluster head is used to aggregate the data from other nodes and send the aggregated data to Base station.During the creation of network topology, the process of setting up routes in WSNs is usually influenced by energy considerations, because the power consumption of a wireless link is proportional to square or even higher order of the distance between the sender and the receiver. In hierarchical routing architecture, sensor nodes self-configure themselves for the formation of cluster heads. In this paper, the survey on energy efficient and secure routing protocol in wireless sensor network and few of them are compared and evaluated.*

Keywords:WSN, Secure WSN, Energy Efficient WSN, Hierarchical routing, cluster head.

1. Introduction

A wireless sensor network (WSN) is a network system composed of geographically distributed devices using wireless sensor nodes to observe physical or environmental conditions, such as sound, temperature, and motion. The individual nodes are capable of sensing their environments ,processing the information data locally, and sending data to one or more collection points in a WSN [1]. Efficient data transmission is one of the most important issues for WSNs. Meanwhile, many WSNs are deployed in harsh, neglected ,and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings [2]. Secure and efficient data transmission is, thus, especially necessary and is demanded in many such practical WSNs [1].

1.1 Low-Energy Adaptive Clustering Hierarchy Centralized(LEACH-C):In LEACH-C, base station is responsible for cluster formation, unlike LEACH where nodes self-configure themselves into clusters [2]. Initially in the LEACH-C, the Base Station (BS) receives information regarding the location and energy level of each node in the network. After that ,using this information, the BS finds a predetermined number of cluster heads and configures the network into clusters. The cluster groupings are chosen to minimize the energy required for non-cluster-head nodes to transmit their data to their respective cluster heads. The improvements of this algorithm compared to LEACH are the following:

*i)*The BS utilizes its global knowledge of the network to produce clusters that require less energy for data transmission [2].

ii) Unlike LEACH where the number of cluster heads varies from round to round due to the lack of global coordination among nodes, in LEACH-C the number of cluster heads in each round equals a predetermined optimal value [2].

1.2 IBS Scheme for CWSNs [1]

An IBS scheme implemented for CWSNs consists of the following operations, specifically, setup at the BS, key extraction and signature signing at the data sending nodes, and verification at the data receiving nodes:

i) Setup. The BS (as a trust authority) generates a master key msk and public parameters param for the private key generator (PKG), and gives them to all sensor nodes.

ii) Extraction. Given an ID string, a sensor node generates a private key sekID associated with the ID using msk.

iii) Signature signing. Given a message M, time stamp tand a signing key _, the sending node generates asignature SIG.

iv) Verification. Given the ID, M, and SIG, the receiving node outputs “accept” if SIG is valid, and outputs“reject” otherwise.

1.3 IBOOS Scheme for CWSNs [1]

An IBOOS scheme implemented for CWSNs consists of following four operations, specifically, setup at the BS, key extraction and offline signing at the CHs, online signing at the data sending nodes, and verification at the receiving nodes:

i) Setup. The BS (as a trust authority) generates a master key msk and public parameters param for the private key generator (PKG), and gives them to all sensor nodes.
ii) Extraction. Given an ID string, a sensor node generates a private key sekID associated with the ID using msk.
iii) Offline signing. Given public parameters and timestamp t, the CH sensor node generates an offline signature SIG offline, and transmits it to the leaf nodes in its cluster.
iv) Online signing. From the private key ID, SIG offline and message M, a sending node (leaf node)generates an online signature SIG online.
v) Verification. Given ID, M, and SIG online, the receiving node (CH node) outputs "accept" if SIGonline is valid, and outputs "reject" otherwise.

2. Related Works

In [1], the authors study a secure data transmission for cluster-based WSNs (CWSNs),where the clusters are formed dynamically and periodically. The author propose two secure and efficient data transmission (SET) protocols forCWSNs, called SET-IBS and SET-IBOOS, by using the identity-based digital signature (IBS) scheme and the identity-based online/offline digital signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in thepairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while itssecurity relies on the hardness of the discrete logarithm problem. The authors show the feasibility of the SET-IBS and SET-IBOOS protocols withrespect to the security requirements and security analysis against various attacks. The calculations and simulations are provided toillustrate the efficiency of the proposed protocols. The results show that the proposed protocols have better performance than theexisting secure protocols for CWSNs, in terms of security overhead and energy consumption.
In [3], the authors present a survey that is focused on the energy consumption based on the hardware components of a typical sensor node (2009). They divide the sensor node into four main components: a sensing subsystem including one or more sensors for data acquisition, a processing subsystem including a micro-controller and memory for local data processing, a radio subsystem for wireless data communication and a power supply unit. Also the architecture and power breakdown as the solution to reduce power consumption in wireless sensor networks is discussed.
In [4], the design issues of WSNs and classification of routing protocols are presented (2009). Moreover, a few routing protocols are presented based on their characteristics and the mechanisms they use in order to extend the network lifetime without providing details on each of the described protocols.
The Authors in [5] presents the challenges in the design of the energy-efficient Medium Access Control (MAC) protocols for the WSNs (2009). Moreover, it describes few MAC protocols (12 in total) for the WSNs emphasizing their strengths and weaknesses, wherever possible. However, the paper neither discusses the energy-efficient routing protocols developed on WSNs nor provides a detailed comparison of the protocols. Our survey is concentrated on the energy-efficient routing protocols discussing the strengths and weaknesses of each protocol in such a way as to provide directions to the readers on how to choose the most appropriate energy-efficient routing protocol for their network.
In [6], few energy-efficient routing techniques for Wireless Multimedia Sensor Networks (WMSNs) are presented (2011). Also the authors highlight the performance issues of each strategy. They outline that the design challenges of routing protocols for WMSNs followed by the limitations of current techniques designed for non-multimedia data transmission. Further, a classification of recent routing protocols for WMSNs is presented.
The survey in [7], presents a top-down approach of several applications and reviews on various aspects of WSNs (2008). It classifies the problems into three different categories: internal platform and underlying operating system, communication protocol stack, network services, provisioning, and deployment. However, the paper neither discusses the energy efficient routing protocols developed on WSNs nor provides a detailed comparison of the protocols
In [8], the authors propose and evaluate clustering technique called a Developed Distributed Energy-Efficient Clustering scheme for heterogeneous wireless sensor networks. This technique is based on changing dynamicallyand with more efficiency the cluster head election probability.Simulation results show that our protocol performs better thanthe Stable Election Protocol (SEP) by about 30% and then theDistributed Energy-Efficient Clustering (DEEC) by about 15%in terms of network lifetime and first node dies.
In [9], authors provide a systematical investigation of current state-of-the-art algorithms (2007). They are classified in two classes that take into consideration the energy-aware broadcast/multicast problem in recent research. The authors classify the algorithms in the MEB/MEM (minimum energy broadcast/multicast) problem and the MLB/MLM (maximum lifetime broadcast/multicast) problem in wireless ad hoc networks.

3. Comparative Analysis of Secure and Energy Efficient Hierarchical Routing

3.1Parameter Value

Network Field	100 × 100 m
N(Number of Nodes)	100
Initial Energy	1 J
Eelec(E.Dissipation for ETx &ERx)	50 nJ/bit
εfs(free space)	10 pJ/bit/m^2
εmp(Multipath fading)	0.0013 pJ/bit/m^4
EDA(Energy Aggregation Data)	5 nJ/bit/signal
Esig	77.4 μJ/signature
Eoff	5 μJ/signature
Eon	12.37 μJ/signature
Data Packet Size	4000 bits
Tool used for implementation	MATLAB 7.6.0

1. Initially, base station is centralized and 100 nodes are setup in a particular region (100 x 100) and each node has equal energy (0.5 joules).
2. In round 1, Cluster Head will be created according to probability condition.
3. The decision of each node to become cluster head is taken based on the suggested percentage of cluster head nodes *p*. A sensor node chooses a random number, *r*, between 0 and 1. If this random number is less than a threshold value, *T (n)*, the node becomes a cluster-head for the current round. The threshold value is calculated based on an equation that incorporates the desired percentage to become a cluster-head, the current round, and the set of nodes that have not been selected as a cluster-head in the last (1/*p*) rounds, denoted by G. *T (n)* is given by:

For Leach-C, the cluster head selection formula is:

$$T(n) = \begin{Bmatrix} \frac{p}{1-p*\left(r \bmod \frac{1}{p}\right)} & if\ n \in G \\ 0 & otherwise \end{Bmatrix} (1)$$

And, for IBS and IBOOS, the cluster head selection formula is:

$$T(n) = \frac{p}{1 - p \times \left(r \bmod \left[\frac{1}{p}\right]\right)} \cdot \frac{E_{cur}(n)}{E_{init}(n)} \forall n \in G_n \qquad (2)$$

$$T(n) = \qquad 0 \qquad \forall n \in !\ G_n$$

Where, E_{cur} is current energy of a particular node and $E_{init}$is initial energy of a particular node.

Optimal number of cluster heads is estimated to be 10% of the total number of nodes.

4. Then, Nodes sends the data to their respective cluster heads and energy consumption will be calculated.

Energy calculation for Nodes in LEACH-C:

If $(dis > d_0)$

$E_{TX} * (d) + E_{mp} * d * (\min\_dis^4)$(3)

If$(dis \leq d_0)$

$E_{TX} * (d) + Efs * d * (\min\_dis^2)$ (4)

WHERE, d_0 is given by:$d_0 = \sqrt{\epsilon_{FS}/\varepsilon_{TR}}$

Energy calculation for Nodes in IBS:

If $(dis > d_0)$

$E_{TX} * (d) + E_{mp} * d * (\min\_dis^4) + E_{sig}$ (5)

If $(dis <= d_0)$

$E_{TX} * (d) + Efs * d * (\min\_dis^2) + E_{sig}$ (6)

Energy calculation for Nodes in IBOOS:

If$(dis > d_0)$

$E_{TX} * (d) + E_{mp} * d * (\min\_dis^4) + E_{on}$ (7)

If $(dis <= d_0)$

$E_{TX} * (d) + Efs * d * (\min\_dis^2)$+$E_{on}$ (8)

5. Cluster Head will aggregate the data and send it to the base station and energy consumption will be calculated for each node and cluster heads.

Energy calculation for Cluster Head in LEACH-C and IBS:

If (dis > d_0)

$(E_{TX} + E_{DA})*(d) + E_{mp}*d*(\min\_dis^4)$ (9)

If (dis<= d_0)

$(E_{TX} + E_{DA})*(d) + Efs*d*(\min\_dis^2)$ (10)

Energy calculation for Nodes in IBOOS:

If $(dis > d_0)$

$(E_{TX} + E_{DA}) * (d) + E_{mp} * d * (\min\_dis^4) + E_{off}$ (11)

If $(dis \leq d_0)$

$(E_{TX} + E_{DA}) * (d) + Efs * d * (\min\_dis^2) + E_{off}$ (12)

6. In round 2, the nodes will become cluster heads according to probability conditionT(n).

7. After selection of cluster heads, Nodes sends the data to their respective cluster heads, that will be selected according to the minimum distance of a particular node from cluster heads and energy consumption will be calculated.

8. Cluster Head will aggregate the data and send it to the base station and energy consumption will be calculated.

9. This process will be repeated until the whole network gets down or number of rounds finished.

10. Performance will be evaluated according to parameters like network lifetime, energy dissipation, no. of data packets sent etc.

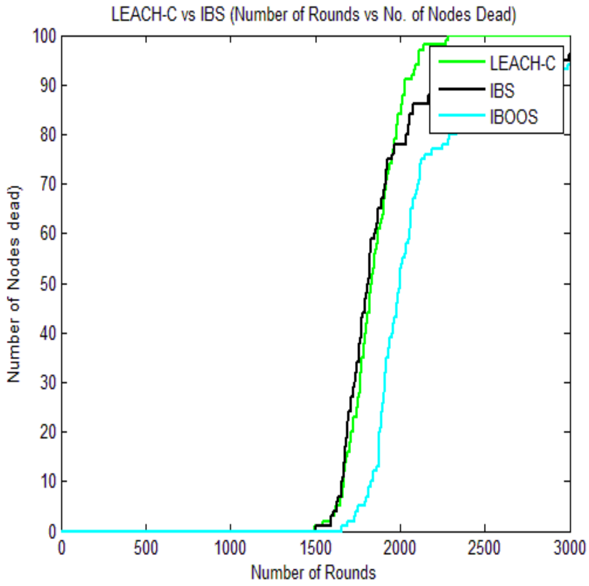

Figure 1: Number of nodes dead vs number of rounds

Figure 1shows the comparison of routing protocols LEACH-C, IBS and IBOOS in terms of Number of nodes dead. Figure1 shows the overall lifetime of the network. Here, we can observe that IBS and IBOOS perform better as compared LEACH-C.

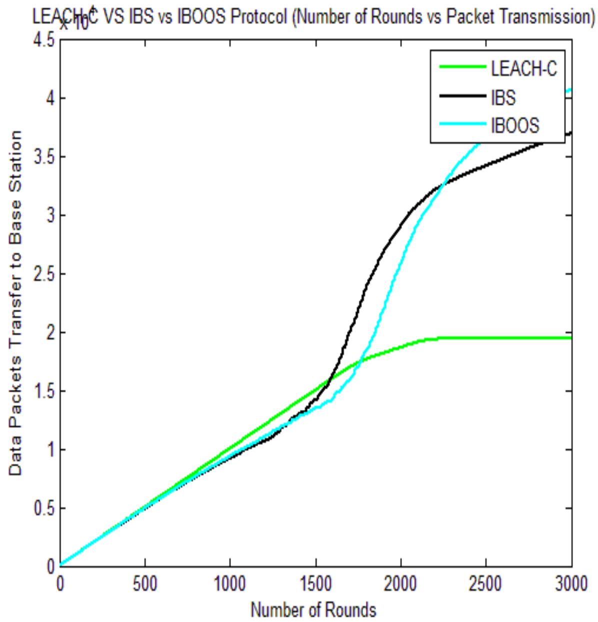

Figure 2: Data packets sent to Base station vs number of rounds

Figure 2shows the comparison of routing protocols LEACH-C, IBS and IBOOS in terms of Data packets sent to base station.Here, we can observe that IBS and IBOOS perform better as compared LEACH-C in terms of Data transfer.

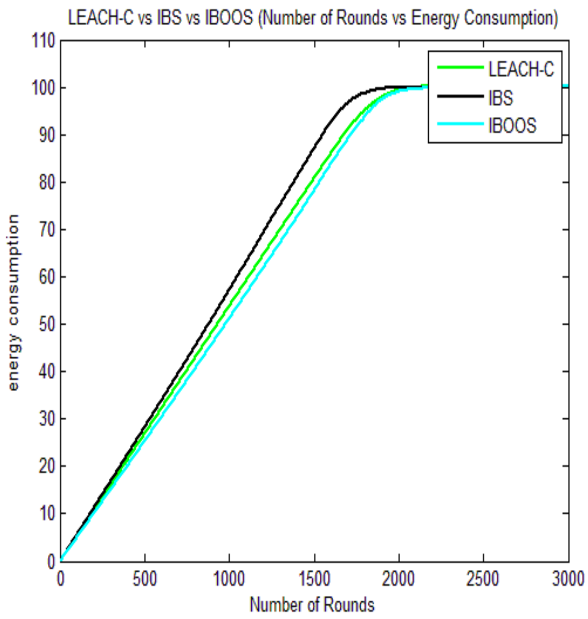

Figure 3: Energy Consumption vs number of rounds

Figure 3 shows the comparison of routing protocols LEACH-C, IBS and IBOOS in terms of energy consumption. Figure 3 shows the overall lifetime of the network. Here, we can observe that IBS, LEACH-C and IBOOS consumes comparatively similar amount of energies.

4. Conclusion and Future Work

A sensor network is composed of many sensor nodes which are deployed in a wide area. These nodes form a network by communicating with each other either directly or through other nodes. One or more nodes among them will serve as sink(s) that are capable of communicating with the user either directly or through the existing wired networks.

One of the most critical issues in wireless sensor networks is represented by the limited availability of energy on network nodes, thus, making good use of energy is necessary to increase network lifetime and increase the efficiency in the performance of routing protocols. In hierarchical routing architecture, sensor nodes self-configure themselves for the formation of cluster heads that cluster head is used to send data packets from or to the main base station. The proposed work is to design a routing protocol which is secure and energy efficient in terms of networklifetime and result will be compared with other IBS,IBOOS and LEACH-C.

5. REFERENCES

[1] Huang Lu, “Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 3, MARCH 2014.

[2] Nikolaos A. Pantazis, Stefanos A. Nikolidakis and Dimitrios D. Vergados, “Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey” IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER 2013.

[3] G. Anastasi, M. Conti, M. Francesco, A. Passarella,“Energy Conservation in Wireless Sensor Networks: A survey,” *Ad Hoc Networks*, 2009, Vol. 7, Issue 3, pp. 537-568.

[4] R.V.Biradar,V.C.Patil,S. R. Sawant,.R..Mudholkar, “Classification and Comparison of Routing Protocols in Wireless Sensor Networks,” *Special Issue on Ubiquitous Computing Security Systems*, 2009, Vol. 4, Issue 2, pp. 704-711.

[5] R. Yadav, S. Varma, N. Malaviya, “A Survey ofMAC Protocols for Wireless Sensor Networks,” *UbiCC Journal*, 2009, Vol. 4, Issue 3, pp. 827-833.

[6] S. Ehsan, B. Hamdaoui, “A Survey on EnergyEfficient Routing Techniques with QoS Assurances for Wireless Multimedia Sensor Networks,” *IEEE Commun. Surveys Tuts.*, 2011, Vol. 14, Issue 2, pp.265-278.

[7] J. Yick, B. Mukherjee, D. Ghosal, “Wireless Sensor Network Survey,” *Computer Networks*, 2008, Vol. 52, Issue 12, pp. 2292-2330.

[8] BrahimElbhiriet. Al. “Developed Distributed Energy-Efficient Clustering (DDEEC) for heterogeneous wireless sensor networks”, IEEE 2010.

[9] S. Guo, O. Yang, “Energy-Aware Multicasting in Wireless Ad hoc Networks: A Survey and Discussion,” *Computer Communications*, *Elsevier*, 2007, Vol. 30, Issue 9, pp. 21292148.