2015

Innovative Self-Organization Wireless Sensor Networks for Electrical Power Systems

Hiu Fai Chan
Hong Kong Institute of Vocational Education (Tsing Yi), Vocational Training Council, chflouie@vtc.edu.hk

Heiko Rudolph
School of Electrical and Computer Engineering, Royal Melbourne Institute of Technology University, heiko.rudolph@rmit.edu.au

Innovative Self-Organization Wireless Sensor Networks for Electrical Power Systems

Mr. CHAN, Hiu Fai
Department of Engineering
Hong Kong Institute of Vocational Education
chflouie@vtc.edu.hk

Dr. RUDOLPH, Heiko
School of Electrical and Computer Engineering
RMIT University, Melbourne, Australia
heiko.rudolph@rmit.edu.au

Abstract
Wireless Sensor Networks (WSNs) gather information for electrical power systems and help to manage demand response and demand side strategies. Optimization of WSNs depends on their physical deployment, and it will bring to the fore a very focused number of parameters to be optimized. Self-organization of WSNs is an important issue to be considered, and it requires the nodes to form a network by collaboration with each other without using manual intervention. Moreover, the WSNs implemented in electrical power systems should be secured and energy efficient in order to provide highly reliable data for monitoring and control.

In this paper, we will propose Self-Organization WSNs with Security and Energy-efficient Clustering algorithms (SOSEC) including cluster formation, data encryption keys establishment and management, and an energy efficient routing protocol. SOSEC can optimize the energy efficiency of the whole network and ensure a secured channel for data transmissions in WSNs for electrical power systems.

Keywords
Electrical Power System, Wireless Sensor Network, Security, Energy Efficient

1. INTRODUCTION

The installation and maintenance costs of traditional wired electrical power system for monitoring and diagnostic systems are relatively high, and change is costly.

Low-cost and reconfigurable WSNs have made it feasible to embed them in electric utility monitoring and diagnostic systems [1]. WSNs can be deployed rapidly and cheaply in difficult terrain to monitor equipment and devices in electrical power systems.

Electrical power systems can be improved by flexible and low cost WSNs [2]. WSNs allow a greater reach of monitoring and thus a faster response to prevent system failures. The scale and wide deployment is not easily achieved with traditional power grid monitoring systems [3]. An electrical power system with WSN system can outperform the traditional one by providing the necessary on time and accurate information through the bi-directional information communication between the electricity suppliers and consumers [4]. WSNs extend the reach of monitor and control points of power generation, transmission, distribution, substations, and consumer sites in order to make the implementation and communication of the whole electrical power systems more efficient and reliable [5].

However, security is one of the most important issues for data communications in the WSNs because personal, financial and infrastructure information are involved during the transactions and transmissions [2].

It should be pointed out that hundreds or even thousands of wireless sensor monitoring sensor nodes are deployed in electrical power systems. The sensors are powered by battery, and they are usually installed on the poles along the transmission lines where are difficult to access. Therefore, the design of the routing algorithms should be energy efficient in order to maximize the life time of the whole WSN system.

2. BACKGROUND

2.1 WSNs Applications in Electrical Power System

WSNs are used in various applications and stages in electrical power systems: power generation, power transmission, power substation, power distribution, and power consumption.

In the power generation stage, generators are the main devices in the power plants. So, flexibly deployable sensors are useful to collect generation data to ensure safety and security [6]. Different types of sensors such as balance sensors, smoke sensors, and magnetic field strength sensors are required to collect data and monitor the status of the power generators. Such information can assist with fault detection, prevent accidents, and optimize the performance of the power generation schedule.

WSNs are especially useful for monitoring the operations of transmission lines and substations, these areas are difficult and expensive to monitor by using traditional methods [7].

Currently, the safety of huge number of power transmission towers relies on regular inspections by patrol officers. This is time consuming, and whenever

faults or disasters occur, it is hard to obtain accurate data for analysis [8]. WSNs can be used on transmission towers to monitor environmental conditions, such as wind direction and speed, vibrations, temperature, humidity, pressure, etc.

2.2 WSNs Security Requirements

Security is a major concern in the data transmissions of the electrical power system through WSNs. A secured WSN needs to fulfill the following requirements:

Data Confidentiality: Preventing sensitive information accessed by unauthorized parties.
Data Authentication: Receiving node needs to make sure that the data is originated from the correct source.
Data Anonymity: The identity of the sending node should not be identified from the data.
Data Integrity: Data must not be altered accidentally or deliberately during transmissions between sensor nodes.
Data Freshness: Data must be recent, and no old messages are replayed by an attacker.

2.3 Data Encryption Methods

There are two major encryption methods: Symmetric and Asymmetric key encryptions.

Symmetric key cryptography uses one private key for encryption and decryption. On the contrary, Asymmetric key cryptography uses a pair of public and private keys to encrypt and decrypt messages. Each node will keep a secret private key itself, and its public key will be known by the authorized receiver.

Both Symmetric and Asymmetric cryptographic algorithms offer advantages and disadvantages. Symmetric encryption provides cost-effective and efficient methods of data encryption, but its encryption method is less complicated. Also, its security level is lower because of using identical symmetric keys for data encryptions between the communication parties. Asymmetric algorithms can ensure higher security based on the more complicated encryption logic and the secrecy of the private key, but it will consume more power.

2.4 Different Clustering Routing Algorithms in WSNs

The chain topology based WSN is not suitable for data communications in electrical power systems because a failure or dead node may hinder the data transmissions for the whole network. The chain topology is not the most energy efficient because data is transmitted by through all nodes in sequence [9]. In this paper we propose a self-organization clustering WSNs, SOSEC, which has security and energy considerations built in.

Clustering is a commonly used data communication technique to reduce the energy consumption by sending data from sensors to base station (BS). In hierarchical clustering, the whole sensor network is divided into different clusters or multiple layers. The transmission within a cluster is coordinated by each cluster head.

Nodes are classified into clusters which are managed by a cluster head. The cluster head is responsible for data routing between clusters and or base station. Data is transmitted through multi cluster heads instead of sending to the base station directly by individual nodes. This can save energy for transmissions over larger distances, and hence improve the lifetime of the whole WSN.

Existing clustering routing algorithms are:

- Low Energy Adaptive Clustering Hierarchy (LEACH),
- Threshold Sensitive Energy Efficient Sensor Network Protocol (TEEN)
- Hybrid, Energy-Efficient Distributed Clustering (HEED)

LEACH is the commonly applicable clustering algorithm for designing energy efficient WSNs which is aimed to reduce the power consumption over the whole WSN. For LEACH, the selection of cluster heads are selected randomly [10] and rotated among the nodes in a cluster based on specific period of time. Each cluster head will gather the data for its cluster and transmit to the base station directly.

TEEN is a hierarchical clustering protocol. It also divides sensors into groups which are coordinated by cluster heads. Moreover, the sensors are divided into multiple levels or layers. In each cluster, members send data to their corresponding cluster heads. The cluster heads then send the aggregated data to the next higher level cluster heads, and until the base station is finally reached.

HEED takes residual energy into consideration when forming clusters. It can help to balance the energy loading among different sensor nodes. HEED is implemented in multi-hop networks. It is expected to maximize network lifetime by balancing energy consumption, minimizing control overheads [11].

For HEED, cluster heads are selected based on the main factor of the remaining energy of each sensor node. This information is used for estimating the probability of each node being elected a cluster head.

We have summarized the advantages and drawbacks of different clustering algorithms in Table 1:

Clustering Algorithm	Advantages	Drawbacks
LEACH	• Aggregation technique to combine the original data into a smaller packet size for transmission to save energy and bandwidth • Every node have an equal chance to act as Cluster heads to save energy	• Due to single-hop routing, the cluster heads will consume a lot of energy when they are located far away from the base station and it is not suitable for large scale applications.
TEEN	• Reduce the transmission distance based on multi hop transmission. • Suitable for large scale networks.	• It may not guarantee a fair and uniform cluster heads distribution because the election of cluster heads is selected randomly.
HEED	• Balance the energy loading among different sensor nodes.	• Energy will be used to communicate the information of residual energy.

Table 1: Advantages and Drawbacks of Different Clustering Algorithm

3. Proposed Self-Organization WSNs (SOSEC)

In this paper, we will propose a Self-Organization WSN with Security and Energy-efficient Clustering algorithm (SOSEC) to optimize the energy efficiency of the whole network and ensure a secured channel for data transmissions in WSNs for electrical power systems.

3.1 Assumptions of Our WSN Model

- There is a base station (BS) in the WSN, and its storage, communication and computation resources are unlimited. It is the only certificates issuing agency in the whole network. It generates and stores ID numbers, private & public keys for all sensor nodes.
- The sensors are randomly distributed and static.
- The sensor nodes are grouped into clusters, and there is one cluster head (CH) in each cluster. Cluster members can transmit messages to their cluster head or directly to the BS. CH can then sends data directly to the BS, or though multi-hops by sending data to next CHs, and finally to the BS.
- Each node stores a secret private key generated by the BS for encryption before data transmission.
- CH will store the public keys of its members and other CHs.

3.2 Cluster Formation Algorithm

The cluster formation is based on the remaining energy and distances between nodes. It will use the remaining energy in selecting the cluster head, and the cluster head role will be rotated if its energy is lower than the required level.

The following is the pseudo code of our proposed cluster formation algorithm:

// initialize:
1 *Enter the expected minimum required energy of a cluster head and cluster members*
2 Initialize total number of sensor nodes
3 Initialize the energy of every sensor node to the same constant value
4 Initialize the size of the network area
5 Indicate the location of the base station
6 Randomly distribution of sensor nodes
7 ***Do while*** *1st round of CH selection OR the CH's remaining energy less than the required value*
8 Base station calculates the average energy, Eaverage, of the current network.
9 ***IF*** *Ei – Eaverage > 0* ***THEN***
10 Node i has the chance to be a cluster head and will put into the CH candidate list
11 ***Else***
12 Not eligible for election
13 // End If
14 ***Loop*** *// end of DO WHILE loop*
15 Extract the sensor nodes from the cluster head candidate list
16 Calculate the number of nodes within the optimal cluster area.
17 Update the cluster heads candidate list
18 Measure the centrality by calculating the cumulative distances from the candidate members and the cluster head
19 Measure the proximity to the data sink by calculating the cumulative distance from the cluster head to the data sink
20 The candidate with highest eligibility value will be the cluster heads.
21 ***FOR*** *every sensor node*
22 Calculate its distance between all cluster heads
23 ***NEXT***

24 The sensor node will join the cluster with the shortest distance
25 Update the membership of the clusters
26 ***IF*** *(the number of sensors within a cluster exceeds the maximum member size)* ***THEN***
27 Assign one more cluster head for the group based on the candidate list
28 // end if

3.3 Multi-Hop Routing Algorithm

If sensor node is close to the base station, it can send data to the base station directly. Besides, we divide the network into multiple clusters where the cluster head node collects and aggregates information from its neighbors and delivers the summary through minimum number of hops to the base station to avoid redundant transmissions and save communication costs.

The following is the pseudo code our proposed routing algorithm:

1 ***FOR every cluster head after a fixed period of time or with certain message size***
2 ***IF*** *the distance to the BS is shorter than other CHs*
3 Data will be sent to BS directly
4 ***ELSE***
5 Extract the cluster heads information from the database
6 Select the next cluster head within the energy efficient transmission range and with minimum hop counts
7 Estimate the energy used for data transmission of both cluster heads
8 ***IF*** *the remaining energy is enough for both cluster heads.*
9 Send the data
10 Update the remaining energy of the cluster heads
11 // end if
12 // end if
13 ***NEXT*** *// for loop*

The energy consumed for a sensor to transmit k-bits data over d meters is based on the First Order Radio Model:

$$Etrans(k,d) = E_{elec} * k + E_{fs} * k * d^2, \ d<=d_0 \quad (1)$$
$$Etrans(k,d) = E_{elec} * k + E_{amp} * k * d^4, \ d>d_0 \quad (2)$$

$$d_0 = \sqrt{\frac{E_{fs}}{E_{amp}}} \quad (3)$$

E_{fs}: required energy for amplification of transmitted signals to transmit a one bit in open space

E_{amp}: required energy for amplification of transmitted signals to transmit a one bit in multi path models

E_{elec}: the energy spent in transmitting and receiving data for a sensor's electronics

The energy is consumed for a sensor to receive k-bits data

$$Ereceive(k) = E_{elec} * k \quad (4)$$

3.4 Encryption Key Establishment and Management

As discussed, the WSNs in electrical power systems should be implemented with a certain security level, and at the same time maintain low energy consumption and high efficiency.

If only one encryption key is shared among all nodes in the network, it requires no establishment of additional keys, and the storage costs and energy consumption can also be minimized. However, the security standard will be extremely poor because if any node in the network is captured by an attacker, the whole network will be compromised. Therefore we propose public and private key pairs with minimum interactions between sensors.

3.4.1 System Initialization Stage

Every sensor node is equipped with a GPS module to collect its own location information, and it can also calculate its own remaining energy.

The base station broadcasts a connection invitation message to all sensor nodes in its receiving range. If the sensor node wants to join the base station, it will generate a one-time session key by a secret random value, and send a connection request message to the base station together with its session key, location and remaining energy information.

After the base station receives the connection request message, it will generate a new ID, a pair of private/public keys based on a secret random value and the node's location information. It will then create a new member record in its database and send the information listed below for encryption by the session key to the connection requested node.

- ID of the connection requested node
- Private key of the connection request node
- The ID and the public key of the proposed joining CH
- Public key of the base station

The private key is only known by the individual sender node, and is used for individual authentication and secure communication assurance. On the contrary, public keys will be selectively sent to authorized receivers.

The sensor node needs to reply with a connection finish message encrypted together with the session key and the BS's public key to the base station.

After the base station received the connection finish message, it will decrypted it with its private key, and check the message, the node is then eligible to send data in the WSN. The base station will then delete the session key and update the status of the node in the database. If no acknowledgement is received within a specific period of time, the connection is declined, and a new connection procedure is required.

If the sensor node is selected as a cluster head, the base station will inform the cluster head with the following information encrypted with the session key:

- ID and private key of the cluster head
- IDs and public keys of the nodes joining its cluster
- IDs and public keys of other cluster heads
- Number of next hops count to the BS

3.4.2 Sending Message

Every node will be assigned a specific time slot to send a message to the cluster head. For the rest of the time, the node will sleep to save energy. When a node wants to send a message in its assigned timeslot, it will encrypt the message with its private key together with its ID, and then encrypt it with the public key of its cluster head.

Public_CH{ ID, Public_BS{Private_sender (msg)}}

After the cluster head received the message, it will decrypt the message with its own private key, and check the ID of the sender. If the ID matches with the member list provided by the base station, it will then accumulate the messages from other members in its cluster during the round. Otherwise, it will just drop the message. After the time is over, it will compress the whole message to save the transmission cost, encrypt the whole message with its private key, and transmit it to the next cluster head based on our proposed routing algorithm.

Public_next CH{ ID, Private_CH (accumulated msg)}

After the targeted next cluster head receives the message, it will then decrypt the message with its own private key, and check the ID of the previous CH sender. If it matches the cluster heads list provided by the base station, it will then repeat the process and send the message to the next cluster head(s). If the ID of the sender does not match the list, it will just decline the transmission, delete the message and inform the BS. Otherwise the last cluster head will encrypt the message with the public key of the cluster head, and finally send the message to the base station.

Lastly, the base station will receive the message and decrypt the message with its private key and then decrypt the message with the public key of the last sender, and check if the ID matches with its database. If matched, then it will decrypt the message with the public key of the original sender one by one to get the data. Otherwise, the whole packet will be dropped.

So, with our proposed security mechanism, it can prevent sending data from unrecognised nodes (attackers) because the message will be rejected and deleted if the sender is not in the list and without the signature (encryption with sender's private key), and no further processing is required in order to save the energy consumption. Moreover, it can ensure confidentiality because only the authorized receiver can extract the original message with its private key and nobody else can modify the original without the decryption key. Thus, the message is sent securely. Therefore, our proposed algorithm can achieve data confidentiality, authentication, and integrity of WSNs

3.4.3 New Node joining

When a new node joins, it needs to wait for the next connection invitation message broadcast from the base station, and repeat the procedure outlined before.

3.4.4 Leaving of a Normal Node

If a node wants to leave the sensor network, it needs to send a connection terminate message encrypted with its private key and then with the base station public key to the base station. After the message is received, the base station will verify it, delete the node in the database and inform the corresponding cluster head.

A base station will regularly broadcast a check status message to all nodes. The sensor nodes need to reply to the message with the status of current remaining energy to the base station, if a node cannot response within the time period for a certain number of times, then that node will be treated as dead. In that case, the base station will delete the node and its keys in the database and inform the corresponding cluster head as well.

3.4.5 Change of Cluster Head

The base station will monitor the remaining energy status of each cluster head. If the energy is less than the required level, the base station will re-select the cluster head based on our proposed cluster head selection algorithm, update its database, and inform the new cluster head and cluster members for the change. It will also announce the change to other cluster heads. Hence the keys involved among the parties will be re-distributed.

3.4.6 Simulation and Analysis

The initial settings of the parameters are described in Table 2, and the environments of the WSN are mentioned in Figure 1.

Network size	300 x 300 m
Number of nodes	100 nos.
Initial Energy of nodes	0.5J
Eamp	0.0013pJ/bit/m
Efs	10pJ/bit/m
Eelec	50nJ/bit

Table 2: Initial settings for simulations

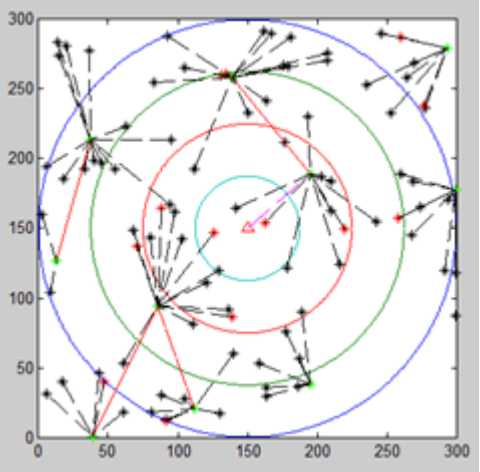

Figure 1: Simulation Environment

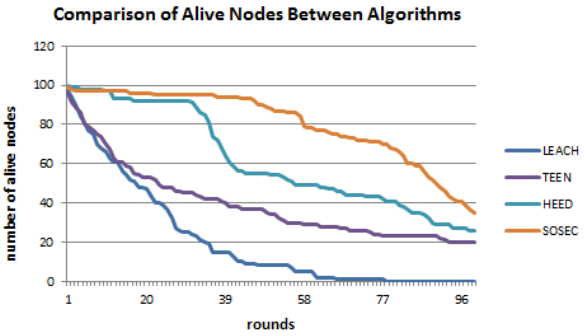

Figure 2: Comparison of Alive Nodes between Different Clustering Algorithms

Based on our simulation and the results obtained in Figure 2, it is found that our proposed SOSEC is better than LEACH, TEEN, and HEED algorithms. There are more total number of nodes still functioning. It is because the transmission distance can be shortened through multi-hop transmissions. Besides, the selection of cluster head is not based on a random number, but depends on the remaining energy level of the nodes and distances. In addition, a node can send data based on minimum multi-hop or send data to the base station directly. Therefore, it can minimize the energy consumption for sending data and encryptions between nodes by reducing the number of transmissions. So, it can improve the network lifetime and also ensure the data confidentiality, authentication, integrity and anonymity during data transmissions with our proposed SOSEC.

4. CONCLUSION

Wireless sensor networks are widely used in different applications nowadays. They can help to enhance the performance and prevent faults in Electrical Power systems. In this paper, we have proposed an energy efficient and secured self-organization wireless sensor network protocol SOSEC for secure data transmission.

References

[1] L. L. Bello, O. Mirabella, and A. Raucea, "Design and implementation of an educational testbed for experiencing with industrial communication networks," *IEEE Transactions on Industrial Electronics*, Vol. 54, No. 6, pp. 3122-3133, Dec. 2007

[2] Y. Yan, Y. Qian, H. Sharif and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications", *IEEE Explore*, vol. 14, no. 4, pp. 998-1010, 2012

[3] D.L. Jia, X.L. Meng and X.H. Song, "Study on technology system of self-healing control in smart distribution grid", *Advanced Power System Automation and Protection*, pp. 26-30, 2011

[4] Y. Van, Y. Qian, H. Sharif and D. Tipper, "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges", *IEEE Explore*, vol. 15, no. 1, pp. 5-20, 2013

[5] Y.X. Yu, "Technical composition of smart grid and its implementation sequence", *Southern Power System Technology*, pp. 1-5, 2009

[6] P. Rodriguez, A. V. Timbus, R. Teodorescu, M. Liserre, and F. Blaabjerg, "Flexible active power control of distributed power generation systems during grid faults", *IEEE Trans. Ind. Electron.*, vol. 54, no. 5, pp. 2583-2592, Oct. 2007

[7] Fangxing Li,Wei Qiao, Hongbin Sun, Hui Wan, Jianhui Wang, Yan Xia, Zhao Xu, Pei Zhang, "Smart Transmission Grid: Vision and Framework", *IEEE Transactions on Smart Grid*, Sept. 2010,pp.l68-177

[8] Lambert, and D. Divan, "A survey on technologies for implementing sensor networks for power delivery systems", *in Proc. IEEE Power Eng. Soc. Gen. Meeting*, Jun. 2007, pp. 1-8

[9] Y. Van, R.Q. Hu, S.K. Das, H. Sharif and Y. Qian, "An Efficient Security Protocol for Advanced Metering Infrastructure in Smart Grid", *IEEE Explore*, vol. 27, no. 4, pp. 64-71, 2013

[10]W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy efficient communication protocol for wireless microsensor networks", *33rd Annual Hawaii International Conference on System Sciences*, 2000, pp.3005-3014

[11] Younis, Ossama, and Sonia Fahmy. "HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks", *Mobile Computing, IEEE Transactions* on 3.4 (2004): 366-379.