# SURVEY ON SECURE ENERGY EFFICIENT ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORKS

[1]Urvashi R. Sharma, [2]Prof. Parth R. Dave
[1] Student, [2]Assistant Professor
[1]Department of Computer Engineering,
Dharmsinh Desai University, Nadiad, India

**Abstract :** In recent years, the use of wireless sensor network has been rapidly increased. As security is an indeed issue of wireless sensor network, provision of security to wireless sensor network for many applications is required. Such applications are health care, traffic surveillance, smart house and most importantly in the defense area. Sensor network plays a pivotal role but security provision is the tip of iceberg in it as security provision leads into more energy consumption. Many secure energy efficient protocols have been introduced over the time to strike a balance between energy efficiency and security provision for sensor network. In this paper, a survey has been carried out to elaborate the efficiency level of different techniques with security measures.

**Keywords: WSN, Energy Efficiency, Security, Authentication, Secure hierarchical protocols**

## I. INTRODUCTION

Wireless Sensor Network is composed of number of sensor nodes, which are communicating directly or via intermediate sensor node with each other wirelessly. Each sensor node has three task to perform: sense the input, process the sensed input and transmit. As sensor nodes are tiny constraint devices, they have certain limitations such as constraint resources, routing, security, reliability and scalability. In addition to that, they have constraint resources in terms of storage, battery power and processing power.

As the battery of sensor node cannot be replenished and cannot be recharged once it is drained, the lifetime of the Wireless sensor network is compromised. There are chances of node failures and mobility mechanism, hence routing becomes one of the important challenge in it. Security is major issue of wireless sensor network as the data or message transmission between nodes and base station is done through the wireless medium. There are many security goals needs to be achieve in wireless sensor network such are data confidentiality, data integrity, data freshness, availability and authentication [1][2].

To achieve these security goals many security techniques are implemented to identify, restrict and recover from the attacks [3]. There are different types of attacks possible on routing protocols of WSNs such are alter, spoof and replay routing information, sinkhole, Sybil, selective forwarding, black hole and hello flooding attack [2]. Security techniques for sensor network are mainly classified in to two types: low level and high-level security techniques. Using cryptographic and hashing functions, low-level security can be provided. Using Intrusion Detection Systems (IDs) , high-level security can be provided but security provision to sensor nodes using cryptographic and intrusion detection system is again an- other challenging task as energy efficiency is another key factor to be taken care within the security for the efficiency of the WSN.

For sensor network, many protocols have been introduced to overcome the issue of security but to achieve security and energy efficiency both, secure hierarchical routing protocols are used in wireless sensor network as secure hierarchical routing is a sequential process that guarantees the security goals in each phase by using cluster formation phase and transmission of data phase. Cluster head selection and assignment of nodes to cluster heads is done during the cluster formation phase and collected data is protected when it is transferring from nodes to the base station by performing data aggregation and data routing to base station during the transmission of data phase. The rest of the paper is organized as follows: Section II provides literature survey with brief introduction about various secure energy efficient protocols and comparison of them. Section III concludes the paper.

## II. LITERATURE SURVEY

### LHA-SP

LHA-SP protocol is based on securing heterogeneous hierarchical wireless sensor network with arbitrary of levels, in which symmetric key scheme is used [2]. In this protocol, each message exchange is encrypted using the group key and the decryption of the message is also done by the same group key. For the integrity of the message, Message authentication code (MAC) is used [4].

**Secure Routing Protocol for Sensor Network**

SRPSN is a protocol propose by Tubaishat et. al., it is the first hierarchical routing protocol that is designed to address secure routing in sensor network from the inception of the network [9]. For secure data transmission, it uses two level hierarchical routing with group key management scheme, which includes group communication policies and group membership requirements for the generation of distributed group key [5][6].

**Security-LEACH**

SLEACH stands for secure based LEACH. It is first protocol, which added security features using SPINS protocol in LEACH [1]. In this protocol, two types of keys are used: master key and group key. Master key is shared with the base station and the group key is shared by the all nodes. One counter is maintained by each node and shared with the base station for the freshness of the data. Whole protocol is executed in to two phase as the LEACH protocol. After the completion of cluster head selection in the set-up phase, a cluster head nodes broadcast a message concatenated with its id and a MAC value produced using the group key. After receiving all broadcast messages from nodes, base station authenticates received broadcasted messages using TESLA broadcast authentication protocol symmetric key building block. Next step is list of authenticated cluster heads is broadcasted by the base station, which is encrypted by MAC with the help of group keys of authenticated cluster head. Then the cluster formation is done in the similar manner as the LEACH protocol and time slots are assigned to their cluster members. After the completion of cluster formation, the steady state phase starts and each node sends their sensed data to the CH, according to their TDMA schedule. The message contains sensor node id, MAC of the sensor node and counter [1]. It prevents sinkhole, selective forwarding and HELLO fooding attacks and it gives effective solution to protect from outsider attack [5].

**Secure Hierarchical Energy Efficient Routing protocol**

SHEER provides energy efficiency and security both. For security, it uses HIKES for key distribution and authentication. For energy efficiency, it implements a probabilistic transmission mechanism. Execution of SHEER protocol is divided in to four phases: an initiation phase, neighbor discovery phase, clustering phase and data message exchange phase.

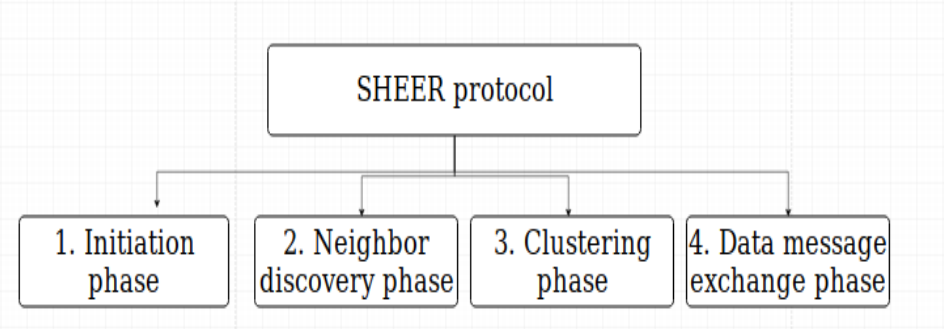


Fig.1 Phases of SHEER protocol

- After deployment of the network, during the initiation phase, a secure initiation call is made for sensor node by base station using HIKES authentication broadcast mechanism as HIKES authentication broadcast mechanism pre- vents an outsider adversary from impersonating the base station [2]. Upon receiving the initiation call, a sensor initializes its internal timer and begins the neighbor discovery phase.

- In neighbor discovery phase, sensors establish their neighbor relationships and they switch between listening and transmission mode. Probabilistic mechanism used by sensor nodes to allow sensor to listen for short period (2 to 10 Second) then transmit a HELLO message containing its id, a nonce and a header encrypted with the sensor specific key and awaits to hear from its neighbors [2]. Each sensor can make maximum three HELLOs, first HELLO broadcasts with radius r and if no response is heard from any neighbor then it sends a second HELLO with radius 2r and if again no response is heard, it sends a third HELLO with radius 4r.

- In clustering phase, based on the closeness, cluster head selection is done for certain levels and cluster formation is done. For the first level cluster head selection, a sensor generates a random p, between 0 and 1. To become first level cluster head condition of equation (1) needs to be satisfied by the sensor node. To become second level cluster head, a first level cluster head repeats the same process by the checking the value of p using equation (1). If the first level cluster head hears the base station it confirms itself as a cluster head. Otherwise, it randomly selects one of its neighbor to take its place as a second level cluster head. Once the cluster heads are independently declared, each cluster head sends a token soliciting members to join its cluster [2].

$$\frac{1}{p} < p \qquad (1)$$

- In data message exchange phase, data messages are sent by the sensors to their cluster head, which aggregates them and forwards the result to the base station.

**Sec-LEACH**

Sec-LEACH is another variant of LEACH with security. At the deployment, a large number of key pools and their IDs are generated in this protocol [1]. A ring of key pools is assigned to each node with pair-wise key, which is shared with the BS in pseudo-random fashion. Cluster head selection is done same as the LEACH protocol by the broadcasting of their ids and nonce. After the computation of CHs and IDs by the other sensor nodes, they select the nearest CH and send a join request message [1]. Then cluster heads send a TDMA schedule to their cluster member. The communication between sensors and the cluster head are protected by a same shared key used in the join request message generated by MAC and in this protocol, value computed from the nonce is used to prevent the reply including reporting cycle [1]. The CH aggregates the decrypted message and sends it to the BS using a symmetric key shared with the BS.

**Specification based secure LEACH**

SSLEACH is a generic specification based intrusion detection model [7]. This protocol uses IDs architecture. In this, agent process (AP) is modeled for the collection component for the analysis of audit data. The AP is executed in the nodes and the information namely agent packet (AGPKT) is periodically send to the base station. The agent process identifies the abnormalities in the trans- mission of the nodes. After the identification of abnormalities, it reports these abnormalities to the base station. Based on this report, base station adds the abnormal or malicious nodes to the list namely black list or announcement list (ANL) , which contains the malicious node list is broadcasted to the entire network periodically [7]. This protocol uses two methods for intrusion detection: agent process and specrule [7].

**Lightweight-Secure LEACH**

LS-LEACH is a protocol in which, authentication algorithm is integrated to ensure data integrity, authenticity and availability. It performs many tasks such as authentication, defining threshold for the number of node to node connections during time (t). In this protocol, node authentication is performed by both the cluster head and by the nodes, using private and public key. Private key is shared between the cluster head and base station, which is used when the node becomes cluster head. Group key is shared between all the node and used when the nodes make request to join cluster. Election of the cluster head is done based on the high remaining energy. Election for the next round cluster heads is done before the end of the current round and the wining node is authenticated by the current cluster head to the base station afterward. Then the base station notifies about the cluster heads elected for the next round. The message from the cluster head to base station is encrypted by the MAC algorithm using private key. Base station broadcasts the list of the authenticated cluster heads to all nodes using uTESLA message broadcast authentication mechanism. Once the broadcasting of the authenticated cluster heads are done, nodes can make a joint request to one of the elected cluster head based on the minimum distance parameter [8].

**Multi level secure LEACH**

Multi Level Secure LEACH protocol uses a stream cipher algorithm RC-4 [9], which uses shared symmetric key for the encryption and decryption. Then the static key is replaced by a dynamic key by toeplitiz hash function. In this proto- col, hash function is used for the authentication between cluster head and cluster formation. Before the deployment of sensor network, the sensor nodes must register with base station with pre-shared key. The keys used in the encryption and decryption process of RC-4 is made dynamic using linear feedback shift register. Toeplitz matrix with a public key is used to generate a hash value, which is processed further to get hardware key that is used for X-OR operation in encryption and decryption process. A matrix is formed from the expanded s vector [9]such that the diagonals are constant, which is called the toeplitz matrix. This matrix then multiplied with message matrix and gives a constant values, which is the required hash and it is used as the secret key for RC- 4 algorithm [9].

**XR-LEACH**

XR-LEACH is an another variant of LEACH with security integration. In this protocol, cluster head election is performed and the formation of cluster is done using hybrid way based on residual energy and vicinity of the node. It uses the key management for authentication and XOR function for secure data trans- mission from cluster member to cluster head as cluster member uses XOR data packets with pad to transmit data to its cluster head and cluster head is using the same pad and XOR the received packet again to get the original data packets [10].

**EESRP**

EESRP [11] stands for energy efficient secure routing protocol, which is introduced for utilizing the energy efficiency in secure manner. Execution of this protocol is divided in to the four phases:

1. Initiation phase
2. Cluster head selection phase

3. Attacker node detection phase
4. Energy dissipation phase.

- In initiation phase, simulation parameter are initialized and clusters are formed in the shape of grid. Sink node is located in the center of the network.
- In cluster head selection phase, average energy of the cluster is calculated and the cluster head selection is done based on the node having greater energy than the average energy of cluster and the nearest distance node from the other nodes of cluster. Then some nodes are randomly selected from the network to participate in the current round. Cluster head selection process is done for to find out the cluster heads for the current round among the randomly selected nodes from network. Then the calculation is done to find number of cluster heads, which are lying between the the selected nodes and the base station.
- In attacker node detection phase, each node sends a check packet to its cluster head and then this check packet is further forwarded from cluster head to base station via intermediate cluster heads. After receiving the sent check packet, the receiver node send check packet back to receiver and if check packet is not returned then node sends the information of the cluster head being a faulty node to all of its neighboring nodes in the cluster.
- In energy dissipation phase, the calculation is done for the reduced energy of cluster head and participating node to identify dead nodes via checking energy of node and cluster head is less than or equal to zero [11].

**Energy saving Wireless Sensor Networks using Kerberos**

For providing security to wireless sensor network in energy efficient manner one scheme is proposed, which uses kerberos as a authentication server [12]. In this proposed scheme, authentication of each sensor node is done through the particular kerberos sever of that cluster and then providing the nodes to communicate with the sink node and the base station. Advantages of this proposed scheme are, it can avoid more time and heavy traffic load with less energy consumption and it processes the nodes request at the same time and this will result in less processing delay as well as will save the energy of the processing nodes [12].

| Protocol Name | Authentication Scheme | Energy Efficiency | Confidentiality | Authenticity | Freshness | Integrity |
|---|---|---|---|---|---|---|
| LHA-SP | MAC | Medium | Yes | Yes | | Yes |
| SRPSN | MAC | Good | Yes | Yes | | Yes |
| SLEACH | MAC | Medium | | Yes | Yes | Yes |
| SHEER | HIKES | Good | Yes | Yes | Yes | Yes |
| Seo-LEACH | | Medium | Yes | Yes | Yes | Yes |
| LS-LEACH | uTESLA | Good | Yes | Yes | | Yes |
| Multi-level secure LEACH | Toeplitiz | Good | Yes | Yes | | Yes |
| XR-LEACH | | Good | Yes | Yes | | Yes |
| EESRP | | Good | Yes | | | Yes |
| Energy saving wireless sensor network using kerberos | kerberos | Good | Yes | Yes | | Yes |
| SSLEACH | | Good | Yes | Yes | | |

Fig.2 Comparison of secure energy efficient protocols

## III. CONCLUSION

Security is always a remarkable issue in wireless sensor network. So to catch security and energy efficiency both in wireless sensor network many secure energy efficient routing protocols are introduced. Secure energy efficient routing protocols are using different authentication scheme to achieve security goals in energy efficient manner.

## References

[1] S. K. Singh, S. Member, and P. Kumar, “A Survey on Successors of LEACH Protocol,” vol. 5, 2017.

[2] I. Ouafaa, E. Mustapha, K. Salah-ddine, and E. H. Said, "Secure Hierarchical Routing Protocols in Wireless Sensor Networks : a Comparative Analysis Mohammed-V University in Rabat , Faculty of Science , Rabat , Morocco 2 . Hierarchical Routing Protocols 3 . Security Goals in WSNs," vol. 10, no. 11, pp. 95–108, 2016.

[3] A. C. Yogeesh, S. B. Patil, and P. Patil, "A Survey on Energy Efficient , Secure Routing Protocols for Wireless Sensor Networks," vol. 5, no. 8, pp. 17702–17709, 2016.

[4] L. B. Oliveira, H. C. Wong, and A. A. Loureiro, "LHA-SP: Secure protocols for hierarchical wireless sensor networks," *2005 9th IFIP/IEEE Int. Symp. Integr. Netw. Manag. IM 2005*, vol. 2005, pp. 31–44, 2005.

[5] I. Ouafaa, E. Mustapha, K. Salah-ddine, and E. H. Said, "Secure Hierarchical Routing Protocols in Wireless Sensor Networks : a Comparative Analysis Secure Hierarchical Routing Protocols in Wireless Sensor Networks : a Comparative Analysis Mohammed-V University in Rabat , Faculty of Science , Rabat , Morocco Ibn," no. November, 2016.

[6] H. R. Roopashree and A. Kanavalli, "Study of Secure and Energy Efficient Hierarchical Routing Protocols in WSN," no. June 2014, 2015.

[7] S. R. Kumar and A. Umamakeswari, "SSLEACH : Specification based Secure LEACH Protocol for Wireless Sensor Networks," pp. 1672–1676, 2016.

[8] M. Alshowkan, K. Elleithy, and H. Alhassan, "LS-LEACH : A New Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks."

[9] R. K. Kodali, S. K. Gundabathula, and L. Boppana, "Multi Level Secure LEACH protocol model using," no. August 2014, 2015.

[10] J. Joshi, J. Rathod, and K. Wandra, "Performance Enhancement of LEACH for Secured Data Transmission," vol. 10, no. May, pp. 2–5, 2017.

[11] M. Mehra, "Energy Efficient Secure Routing Protocol ( EESRP ) in Wireless Sensor Network," vol. 2, no. 03, pp. 29–33, 2015.

[12] A. Devi, "Energy saving Wireless Sensor Networks using Kerberos," vol. 3, no. 5, pp. 296–298, 2014.