International Journal of Computer Networks and Communications Security

VOL. 2, NO. 11, NOVEMBER 2014, 400–413
Available online at: www.ijcncs.org
ISSN 2308-9830

# Recent Advances of Secure Clustering Protocols in Wireless Sensor Networks

**MOHAMED ELHOSENY[1], HAMDY K. EL-MINIR[2], A. M. RIAD[3] AND XIAOHUI YUAN[4]**

[1, 4] Department of Computer Science and Engineering, University of North Texas, U.S.A.

[1, 3] Department of Information Systems, Mansoura University, Egypt

[2] Department of Electrical Engineering, Kafr El-Sheikh University, Egypt

*E-mail: [1]mohamed.elhoseny@unt.edu, [2]hamdy elminir@eng.kfs.edu.eg, [3]amriad2000@yahoo.com, [4]xiaohui.yuan@unt.edu*

## ABSTRACT

Wireless Sensor Networks (WSNs) have been employed in many real-world applications that greatly improve our life. The ubiquitous WSNs make security a prime issue, and new technologies have been developed recently. In this article, we review the most recent secure clustering protocols in WSNs. We start with a description of the security requirements for WSNs and discuss the existing security schemes. We analyze to what extend they have been applied to the clustering structure of WSNs. Then, we review secure clustering protocols in emerged recent years. Finally, we present a set of criteria which must be applied to build a secure clustering algorithm.

**Keywords:** *Wireless Sensor Networks, Secure Cluster Formation, Secure Routing, Secure data Aggregation, Security Attacks.*

## 1 INTRODUCTION

Wireless Sensor Network (WSN) consists of sensor devices transpired in tangible insecure environments in order to collect data. There have been many applications in health care monitoring, environmental monitoring, industrial logging, etc. The data collected could be sensitive and relevant to privacy, which makes security a prime issue [1], [2]. Unlike conventional networked devices, factors such as open communication medium, limited computational capabilities of nodes, and the disadvantages of bandwidth constraint make WSN more susceptible to malicious attacks [3].

To increase network life and reduce energy consumption, cluster model was proposed [4]. In this model the energy of sensor nodes are reserved by involving them in multi-hop communication within a particular cluster and performing data assembling and fusion as shown in Figure 1. Each cluster has a head node that is responsible for gathering data from all nodes within the cluster and sending the aggregated message to the base station.

There have been reviews on the security procedures and threats of WSNs [5]–[7], and others discuss the procedures related to the clustering model specifically [8]–[11]. However, most of these reviews evaluated the secure clustering algorithms based on two main processes only, i.e., CH selection and cluster formation [10], [12], [13]. Other works discussed the existing secure routing protocols of clustering model with the aim of protecting the data transmission CHs and the base station [8], [14]–[16]. But for any secure clustering algorithm, a set of criteria must be used to be an effective one.

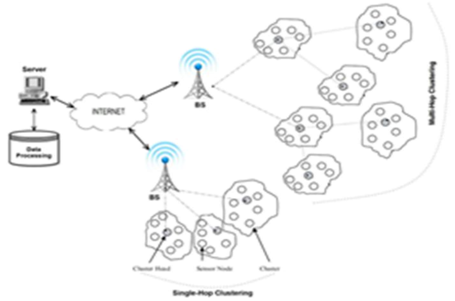

*Fig. 1. Clustering Model for Wireless Sensor Network*

These procedures include secure CH building, secure cluster formation, secure data aggregation from cluster members, secure data routing from CHs to the base station, robustness against different types of attack, efficiency in terms of WSN resources limitations, and ability to deal with dynamic clustering environment. For example, the survey paper [10] considers that all selected algorithms that it explains are secure and efficient. However, they do not pay much attention on energy constraints when different security mechanisms are used. This is very crucial because technique based probabilistic and deterministic strategies have different impacts on energy consumption which will affect the network efficiency and performance directly. In addition, the survey [10] did not address the performance requirements study (e.g. memory requirement, computation overhead etc.), which is more important because it is strictly bound to the consumed energy. Based on that, this work not limited to a specific point in secure clustering, it is an attempt to combine all these processes, i.e., secure cluster building and secure data transmission, as evaluation criteria for some secure clustering algorithm.

The rest of this paper is organized as follows: section 2 review the common types of attacks for WSN and the source of each one. Section 3 explains the evaluation criteria that is used in this paper to evaluate the secure clustering algorithms. Section 4 discusses the most popular security mechanisms which can be used with the clustering model in WSN. Section 5 reviews some of existing secure clustering algorithms with the strengths and the limitations of each one. After that, section 6 analyzes the discussed secure clustering algorithms using the proposed evaluation criteria. Finally, section 7 summarizes the paper.

## 2 SECURITY ISSUES IN WSNs

Security attacks against WSNs can be categorized into two types: active attacks and passive attacks. In passive attacks, attackers are typically hidden and aim to monitor the communication link to collect data. The common examples of passive attacks are eavesdropping, node malfunctioning, node destruction and traffic analysis types. In active attacks, the attacker affects the operations of network, i.e., the transmitted data. For example, the network services may degrade or terminate as a result of these attacks. The common examples of active attacks are Denial-of-Service (DoS), hole attacks, flooding and Sybil types [6]. The source of the attack can come to the network from inside, outside, or both [5]. Table I lists the common types of attack in WSNs.

These attacks aim to affect the transmitted data with one of the following threats [17]:

- Interruption: is an attack on the availability of the network. Its main aim is to make an asset of the system, i.e., sensor node, unavailable or unusable. Denial of Service attacks [5] have become very well-known example of interruption.
- Interception: is an attack on confidentiality. The sensor network can be compromised by the attacker to gain unauthorized access to sensor node or data store within it. Spoofing attack is a well-known example.
- Modification: is an attack on integrity of the system. It this attack unauthorized party not only accesses the data but also modifies the content of a message being transmitted in a network.
- Fabrication: is an attack on authentication in which the attacker make an insertion of messages in a network and tries to make it as it is sent from authorized node.
- Methods to address WSN security attacks aim at the following aspects [18]:
- Preventing Attacks: It aims to prevent any attack before it happens. Any proposed technique will have to defend against the targeted attack.
- Detecting Attacks: If an attacker manages to pass the measures taken by the prevention mechanism, the security solution would immediately switch into the detection phase of the counter attack in progress and specifically identify the nodes that are being compromised.
- Removing Attacks: It aims to mitigate any attack after it happens by removing the affected nodes and securing the network.

## 3 EVALUATION CRITERIA FOR SECURE CLUSTERING IN WSNs

In this section we discuss the criteria which we will use to evaluate the existing secure clustering method.

### A. Completeness

Secure clustering is a sequential process that must guarantee the security goals, i.e. confidentiality, integrity, and availability, in each phase. This process consists of two stages: cluster building and data transmission. The cluster building stage starts with cluster formation in which the cluster heads (CHs) are determined and nodes are assigned to the CHs. The next stage, i.e., data transmission, aims to protect the collected data during its transferring from nodes to the base station. It has two main steps: data aggregation and data routing to base- station. Data aggregation is the process of transmitting data from nodes to the CH inside the cluster. Then CHs forward the data to the base station through a specific path known as routing process. Finally, the base station receives the data and extracts the meaning, and then the process will start again as shown at Figure 2. To achieve secure clustering, these steps shall be enforced. In this paper, we evaluate the existing secure clustering methods and show to what extend each method is. We use S − CH, S − CF , S − DA, and S − DR to indicate to the four phases respectively.

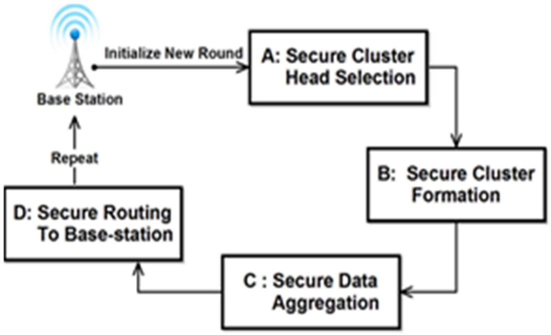
Initialize New Round
A: Secure Cluster Head Selection
Base Station
Repeat
B: Secure Cluster Formation
D: Secure Routing To Base-station
C : Secure Data Aggregation

*Fig. 2. Secure clustering process consists of four steps: Secure Cluster Heads Selection, Secure Clusters Formation, Secure Data Aggregation, and Secure Routing of Data to the base station. The arrows depict data flow.*

### B. Achieving Security Goals

Secure clustering algorithm must achieve the security goals, i.e., integrity, confidentiality, availability, and freshness to avoid attacks and threats as much as possible. These goals can be summarized as the following [19]:

- Integrity: Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized party. To insure that data reaches to the intended receiver without any alteration, a technique like hash function can be used.
- Confidentiality: Confidentiality prevents sensitive information from reaching the wrong party, while making sure that the right party can in fact get it. So, while communicating the data in the network, no one can understood except intended recipient.
- Availability: Availability requires that WSN assets, i.e., data, are available to authorized parties, i.e. CH and base station, at appropriate time and not prevented through this time. It is a requirement intended to assure that WSN work promptly and service is not denied to authorize parties when they request them. So, with availability services of a network should be available always even in presence of an internal or external attacks.
- Freshness: Freshness is a central goal which is violated by replay attacks in which the attacker retransmits an old message to occupy system resources or confusing the receiver, i.e., base station. Generally, it ensures that no old messages have been replayed.

In order to evaluate each of the existing clustering algorithms from the robustness point of view, we will use two notations: P −R and A−R to indicate its work against passive attack and active attack respectively.

### C. Robustness

A secure clustering algorithm must be as robust as possible. The degree of robustness is measured by the count of attacks that the algorithm prevents. It also depends on the kind of attack, whether it is active or passive. The previous list of attacks is used through this paper to evaluate the robustness of each of the secure clustering algorithms.

### D. Efficiency

Secure clustering algorithm must take into consideration the WSN resource limitations, i.e., sensor memory size, energy, and computation powers. That is refers to preventing the complex security procedures that may decrease the network lifetime. It must balance between the security issue and the network performance. This is refers to the efficiency of the secure clustering algorithm. We will evaluate efficiency the secure clustering algorithms using three criteria: required memory (M), energy consumption (E), and the processing time (P ).

### E. Dynamic Clustering

Dynamic clustering process aims to reforming the network structure after each round according to the updated status and characteristics of the sensor nodes, i.e., the remaining energy of each sensor. On the other side, the static clustering algorithm allows only the CH change after each round. It forms the network structure to a fixed set of clusters at the initial round and makes it unchangeable until the network become unavailable, i.e., all nodes consume their energy.

Therefore, we have to find simple solution that allow securing the dynamic cluster network while consuming as little energy as possible and is adapted to a low computing power. This report discuss the existing schemes for secure clustering according to the previous criteria and proposes a complete security schema for routing data between sensors nodes, CHs, and the base station in cluster-based model for WSN.

*Table 1: The Common Types of Attacks of WSN and the Source of Each.*

| Code | Name | Description | Active | Passive | Inside | Outside |
|---|---|---|---|---|---|---|
| A1 | Denial of Service | It sends unnecessary packets and utilizes more network bandwidth to prevents the user from accessing the service or | √ | | √ | √ |
| A2 | Selective Forwarding | It tries to put a malicious node to act as normal node and drop the messages as soon as they receive it. | | √ | √ | |
| A3 | Sinkhole | This attack adds a node to the network to capture all data as if it was the base station. | √ | | √ | |
| A4 | Sybil | The malicious node claims multiple identities to be able communicate with many nodes. | √ | | √ | |
| A5 | Wormhole | This attack records the messages to another location and may retransmit them or a selective part of them. | √ | | √ | √ |
| A6 | HELLO Flood | This attack sends the HELLO packet to the nodes, the node may assumes the attacked device as a neighbor that tries to connect with it. It aims to consume the network resources | | √ | √ | |
| A7 | Spoofed, altered or replayed routing information | This is the most direct attack. By spoofing, altering or replaying routing information the attacker can complicate the network through some actions like create routing loops or generating false error messages. | √ | | √ | √ |
| A8 | Black-Hole | The malicious node communicates the destination node with false route information to enforce it to send the reply to | √ | | √ | |
| A9 | Node Destruction | This attack aims either to make the node unavailable to replace it with a malicious one with the same identifier, or to prevent it from collecting data | √ | | | √ |
| A10 | Monitor and Eavesdropping | This attack aims to gather information about the network. | | √ | | √ |
| A11 | Traffic Analysis | This attack aims to intercept and examine messages in order to deduce information from patterns in communication. Its danger comes from its ability to work even when the | √ | | | √ |
| A12 | Node Replication | This attack creates duplicate nodes and built up various attacks using them nodes. | √ | | | √ |
| A13 | Message Corruption | This attack performs three main actions: receives message, modifies it to be not understandable, and then forwarding it | √ | | √ | √ |
| A14 | Jamming | Jamming interferes with the radio frequencies of the sensor nodes to make them unavailable. | √ | | | √ |
| A15 | Node Malfunction | This attack generates inaccurate part of data that could expose the integrity of the data-aggregating process at the | √ | | √ | |

Table 2 shows the notations for the previous criteria that we use to evaluate the secure clustering algorithms.

## 4 THE EXISTING SCHEMES FOR SECURE CLUSTERING IN WSN

In order to apply security for clustering model, many security procedures such as the data partitioning, using key management, intruder detection by location or trust management [20] have been proposed. Cryptographic techniques, such as encryption and hashing, are useful in addressing these concerns. However, the use of these schemes greatly increases the energy consumption of sensor nodes and thus shortens their lifetime [21] as they need Key management specially in case of using asymmetric key schema. In addition, most of the traditional key management schemes assume the relationship between nodes is fixed, while clusters as well as the relationship between nodes in hierarchical protocol are dynamic, so these schemes designed for flat networks need modifications to be applied for cluster-based WSNs [22]. Furthermore, in asymmetric key schema a larger sensor memory size is required for key storage.

On the other side, Key management scheme (specially symmetric key schema) has two main advantages: it is safer by realization of node-to-node authentication, and it saves energy which is a challenge for any secure protocol [23]. In order to make use of these advantages in clustering model, many dynamic key management techniques were proposed [10], [24]–[27]. In these new schemes a Key is created for each cluster and it will be common among the cluster nodes to guarantee the confidential communication between them. After each round, the cluster key will changed with the changing of the CH. The main problem of these methods is its need for more computation and require more memory size to store the encryption Keys. These requirements affect directly the network lifetime. In the remaining of this section we discuss a list of the existing security solutions, they advantages and their limitations as the following:

*Table 2: The Notations of the Evaluation Criteria for a Secure Routing Protocol*

| Notation | Meaning |
|---|---|
| S-CH | Secure Cluster Head Selection |
| S-CF | Secure Cluster Formation |
| S-DA | Secure Data Aggregation |
| S-DR | Secure Data Routing |
| $A_i$ | Attack Identifier, i.e., $A_1$ means DOS |
| M | The required memory size |
| E | The energy consumption ratio |
| P | The required processing time. |
| D | Dynamic Clustering |
| S | Static Clustering |

### A. Data Partitioning/ Multi-path Routing

In this type of security schemes, the aim is to divide the information into several parts. If a sensor tries to send information, it cuts the data into several packets of fixed size. Each packet is sent on a different route. Packets pass in different nodes. When the packets are received by the sink, it brings them together to regenerate the original message. The main advantage of this method is that: the attacker has to catch all packets of a message if it wants to know the information. In order to do it, it has to be able to listen the entire network. It is more complicated for an attacker to have the information. On the other hand, this solution requires additional computations to collect the different packets to regenerate the message. In addition, it is not suitable for all cases of clustering model. It is also appropriate to the multi-hope clustering model in which a CH communicates with the base station through another CH. In most cases, data partitioning requires an additional security mechanism, i.e., cryptography, to protect the packets during transmission.

### B. Hashing

Hash functions have a very simple purpose, they take a long message and generate a unique output value (called message digest) derived from the content of the message. Message digest can be generated by the sender and transmitted with the message to the receiver which uses the same hash function to recompute the digest. We can exploit the unique properties of hash function as: the input can be of any length, the output has a fixed length, the hash function is one-way, and the hash function is collision free to prevent the active attack that modifies and retransmits the message. In addition, most hash functions produce a 128-bit message digest which represents a solution of the memory size of the sensor nodes.

### C. Cryptography

Due to the resource constraints of wireless sensors, public- key based cryptographic algorithms, i.e., RSA, are too complicated and energy-consuming for WSNs. However the symmetric cryptographic technique has its own qualities that always make it favorable as compared to public key cryptography for WSNs [28]. As a result, most of cryptography solutions in WSN use symmetric key for securing the network, which are more adapted, quicker to perform, and not consume more energy. Although the cryptography allows us to secure the confidentiality of data, its main problem is the key distribution, and we need to find an appropriate key management schema for the network.

According to [11], there are four types of key management techniques which can be used:

1. ***Global key***: In this method, one key is shared by the entire network. To send a message, information is encrypted with this key. Once the message is received, it can be decrypted with the same key. This solution is an energy-efficient solution of cryptography. The information is encrypted once by the sender and decrypted only once by the receiver. However, its the solution with a limited security. If an attacker could find the key, he is able to hear the entire network which communicates with this unique key. To know this key also allows the possibility to insert a malicious node in the network.

2. **Pair wise key node:** Each node has a different key to communicate with a neighboring node which shares this key. So if one node has ”n” neighbors, it has ”n” key stored to communicate with its neighbors. In this solution, a node that sends a message has to encrypt the message with key neighbor who receives the information. The neighboring decrypts information to re-encrypt with the key corresponding to the following receiver. This solution increases considerably the security of the network, because if an attacker discovers a key, this key is just able to communicate with two nodes, and limits the power of this attack. The attacker has to find all pair wise key to listen the entire network. However, this technique is not energy-efficient especially in time of calculation, since each pair of nodes which transmits information has to encrypt and decrypt a message. The lifetime of the network and its rate is going to be reduced. So, we think it may be inefficient solution in case of clustering model because it will consume more energy from the CH in order to decrypt all messages from all sensors inside the cluster. Also, it requires additional memory size for the cluster head to store all keys of all nodes which will be impossible in case of dynamic model.

3. **Pair wise key group:** Each group or cluster has a key to communicate between nodes in the cluster. This solution offers a compromise between security and energy efficiency. It may limit the number of encryption in communications. However it increases the work of clusters heads, which have to decrypt and encrypt the information. To be effective, we have to ensure that CHs change regularly in order not to consume all the energy of the CH. The main advantage of this method is that it can be applied to the dynamic clustering model.

4. **Individual key:** In this solution, each node has its own key to encrypt data. This key is only known by the sink. As a consequence, a message sent by this node goes around hidden on the network until it reaches the sink. This solution is one of the better way to limit the consumption of the network. Nevertheless, this solution secures only communication between a node and the sink. In cluster model, this technique may consume the CH energy rapidly in case of many malicious node attached themselves to the cluster and sent unwanted messages to the CH. In such case, the CH will forward the data automatically to the base station without know its meaning. However, if

we find a method to guarantee that the CH will know the source of the message, i.e. we can use the Node Coordinates as an identifier; this method can be used and represents a good solution.

### D. Generation

Another key distribution solution is to use a key generation. Each round or generation, the sink sends a new key to the whole network. This key is used as a certificate for each node, to prove it belongs to the network. If an unidentified node tries to come into the wireless sensor network and if it does not have this key generation, the network will refuse its integration. Another benefit of this technique is that it limits substitution attacks of a sensor and the reprogramming of the sensor to be reused in the network. This technique is energy-efficient and easy to apply. However it directed only closed networks, which cannot accept new nodes. Moreover, there is the problem of a node, which cannot receive a key to progress time.

### E. Localization

The work of this method is to use a technique for locating a node. For this solution, the wireless sensor network needs specific sensors called beacon node, which are sensors that knowing their geographical position. For example they can use a GPS equipment. The problem is that it cannot work on any other type of sensors.

### F. Intrusion Detection System (IDS)

Intrusion is an unauthorized (unwanted) activity in a net- work that is either achieved passively (e.g., information gathering, eavesdropping) or actively (e.g., harmful packet forwarding, packet dropping, hole attacks). In a security system, if the first line of defense, Intrusion Prevention, does not prevent intrusions, then the second line of defense, Intrusion Detection, comes into play. It is the detection of any suspicious behavior in a network performed by the network members [6].

An IDS is also referred to as a second line of defense, which is used for intrusion detection only; that is, IDS can detect attacks but cannot prevent or respond. Once the attack is detected, the IDSs raise an alarm to inform the controller to take action [7].

## 5 SECURE CLUSTERING ALGORITHMS

In all clustering methods, security and reliability aspects of clustering and cluster head election have gained modest attention so far. On the one hand, there are many papers that survey the security solutions applied in wireless sensor networks, e.g. [6], [8], [11], [17], [26], [29], [30]. These papers detail the common security issues in sensor networks, like authentication, intrusion detection, secure routing, secure data aggregation, etc. However, none of these papers address the issue of secure building and data transmission in particular.

On the other side, some papers, e.g. [31], [32], tackle the problem of secure clustering and secure CH election in sensor networks focusing on issues like dynamic key change, complexity, cluster head election criteria, and so on. Regrettably, the latter papers do not consider the security routing aspects of clustering [29]. In this section, we focus on the existing secure clustering algorithms for WSN as general to evaluate them according to the proposed criteria.

### 5.1 SLEACH

SLEACH protocol is the first attempt to build a secure version of the well-known LEACH protocol. It is prevents sinkhole, selective forwarding and HELLO flooding attacks. SLEACH prevents an intruder node to send falsified data messages. But it doesn't guarantee confidentiality and availability. This algorithm works with homogeneous WSNs in which all nodes have the same characteristics, i.e., initial energy, and processing power. This algorithm makes use of cryptography as the security mechanism by using symmetric-key methods. It can protect the network from outsider attack but it decreased the network efficiency and performance.

### 5.2 SS-LEACH

SS-LEACH [33] is another protocol that offers security while being energy efficient. For that, it works with multi- path CHs to communicate with the base station. To ensure security, it employs key pre-distribution and self-localization techniques. SS-LEACH is protected from selective forwarding, Hello flooding and Sybil attacks, but it controls neither data integrity nor freshness [26]. SSLEACH improves the network efficiency by improving the method of selecting CHs and forms dynamic multi-paths CHs chains to transfer data to the base station.

### 5.3 ESODR

In ESODR [34] method, each cluster is made up of a CH and multiple gateways (GWs) and other cluster members. ESODR combines hash function, symmetric key cryptographic algorithm, and public key cryptographic algorithm together. In ESODR, the computational complexity is low and has got good efficiency and scalability but it suffer from the dynamic clustering nature of the network. In addition, it requires more memory size to store both the encryption key and the hash digest.

### 5.4 SecLEACH

SecLEACH [24] is an improvement of SLEACH. It is a protocol for securing node-to-node communication in LEACH- based networks. It introduced symmetric key and one-way hash chain to provide different performance numbers on efficiency and security depending on its various parameter values. Although it provides authenticity, confidentiality, integrity and freshness for node-to-node communication, SecLEACH did not provide a solution for the compromised CH attack. This is because SecLEACH is vulnerable to key collision attacks and do not provide full connectivity.

### 5.5 RLEACH

RLEACH protocol attempts to apply random pairwise key (RPK) scheme onto LEACH. AS in LEACH, RLEACH operation is round based. It has three basic phases: shared-key discovery phase, cluster set-up phase and data transmission phase. RLEACH has the ability to resist to several attacks such as selective forwarding, sybil and hello flooding. Nevertheless, it is possible that an insider exercises sinkhole attack to be CH. Compromised node can also corrupt BS by the falsified data messages it sends [26].

### 5.6 ORLEACH

The same idea of RLEACH was applied by adding IDS mechanism as a new phase and produced a new method called ORLEACH [4]. ORLEACH operation is, therefore, divided into the following phases: Shared-key discovery phase, Cluster set-up phase, isolation of previously detected, attackers and MNs selection, Data transmission phase and Intrusion detection and alerting phase. Although this algorithm solved the problems of RLEACH specially whose are related to the active attacks, it is complexity increases the processing time and the consumed energy of the network which directly affect its efficiency.

### 5.7 NSKM

NSKM [35] is a secure clustering method that tries to solve the problems related to key management. It provides an efficient key distribution and establishment way by using three categories of keys; pre-deployed keys, network generated keys and the BS broadcasted keys. It works well against replay and node capture attacks. The selection of CH among nodes is based on its location and its distance to base station. NSKM also ensures that the whole network is never compromised even if there has been an attack in the network by providing a secure data routing from CHs to the base station. Its main problem is it cannot work with dynamic clustering environment and suffers from active attacks, i.e., sinkhole and wormhole.

### 5.8 EECBKM

EECBKM [28] is a cluster based technique for key management which the clusters are formed in the network and the CHs are selected based on the energy cost, coverage and processing capacity. An EBS key set is assigned by the base station to every CH and cluster key to every cluster this proposed technique reduces node-capture attacks and efficiently increases packet delivery ratio with reduced energy consumption. But the problem of this protocol is that it works well in the environment with low density of sensors. In addition, it suffers many kinds of active attack. Another method is the SAC which is successful in preventing attacks caused by adversary like hello flooding and provides resilience to sensor nodes captured by adversary [22]. PIKE uses probabilistic techniques to establish pair wise keys between neighboring nodes in the network. However, in this approach, each node has to store a large number of keys.

### 5.9 SCMRP

Another secure clustering algorithm is SCMRP [36] which is based on multipath technique. SCMRP collects the benefits of both cluster based routing and multipath routing. It provides security against various attacks like altering the routing information, selective forwarding attack, sinkhole attack, wormhole attack, Sybil attack etc. In addition, it uses cryptography as a security mechanism to protect message after portioning it to packets. SCMRP consists of five phase; neighbor detection and topology construction, pairwise key distribution, cluster formation, data transmission, and re-clustering and rerouting. The Base station collects all the neighbor list from sensor node and apply an algorithm called DFS for finding multiple path. The BS generates the pairwise key and unicast to all nodes. The CH selection is based on the remaining energy of the node.

### 5.10 SHEER

SHEER [37] aims to create a secure clustering schema with energy-efficient and secure communication on the network layer. SHEER uses the cryptography as the security mechanism. It proposed a schema for key distribution based on the Hierarchical Key Establishment System (HKES). SHEER proposed also a probabilistic transmission mechanism to re- duce energy consumption and extend the network lifetime. This method works effectively against HELLO flood attack, sybil attack and sinkhole attack. Its main drawback is that it is not able to protect the network from selective forwarding attacks.

### 5.11 AKM

AKM [38] is s cryptography-based method that provided security by using two kinds of keys: a pair-wise between the nodes inside the cluster, and a network key. This algorithm provides multiple level of encryption that works well with secure cluster formation and avoid node captures. AKM pro- vides confidentiality, continuous authentication of nodes in the network by periodically changing the network key. However, if the compromised node attached with the network before refreshing the current network key, all the network operations of can be monitored.

### 5.12 SRPSN

SRPSN [39] is another cryptography-based in which a symmetric key is shared between all CHs and the base station to protect data. SRPSN does not guarantee only the cluster building process, but also it is designed to protect the data packet transmission on the sensor networks under different types of attacks. Concerning to the key mechanism, this algorithm used the group key management scheme. However, one of its limitations is that there is no authentication in the mechanism. As a result, SRPSN fail to protect against many types of attacks specially spoofing, altering, replaying and sybil attack. Also, malicious node can also become a sinkhole.

### 5.13 SecRout

SecRout [40] aims to protect the network from compromised nodes attack. The main advantage of SecRout is its ability to detect the data modification if it occurs by malicious nodes during the transmission process. It uses efficient sym- metric cryptography to secure data with two types of keys: the master shared key between the sink and CHs, and the cluster key among the clusters. Also, it guarantees freshness of data which enable it to catch any modified part. Another strength of SecRout is that it uses two-level architecture that reduces the communication overheads between nodes. Therefore, SecRout can greatly save the energy, and decrease the usage of memory and bandwidth.

### 5.14 IKDM

In IKDM [41] each node has a unique identifier (ID) in the network. It uses Pairwise key a mechanism for cryptography. The node ID is assigned at the initialization phase of the net- work by an offline Key Distribution Server (KDS). Then every nodes create a pair-wise key between them by exchanging their node IDs first. This method provides better network throughput and fixed key storage overhead and is suitable for large-scale WSNs. Therefore IKDM scheme is more energy-efficient due to the lower communication overhead for sensor nodes during the pair-wise key establishment process. Also, it can achieve better network resilience against node capture attack.

### 5.15 Genetic Algorithm-Based techniques

In addition to the previous algorithms, a lot of security works based on intelligent techniques, i.e., GA, were proposed. For example, GBSWSHS was proposed at [25] to secure WSN which is used in health care applications. In GBSWSHS method, the actual data is encrypted by using the key which is extracted from the receiver’s fingerprint biometric. Second, to reduce a transmission-based attack, the fingerprint based cryptographic key is randomized by applying a genetic operator. However, the computation time, memory size, and the network lifetime are the main problems of this method. We will exclude GBSWSHS from our analysis because it was proposed as a general security method for WSN which was not created for the clustering model. Another GA based schema was proposed at [42]. This scheme is divided into three parts respectively for the base station, the CHs, and the sensor nodes. The base station first uses GAs to generate appropriate key-generating functions (KGFs) for re-keying on sensor nodes under energy consumption constraints. The functions are further divided into code slices which are then embedded into sensor nodes and headers before deployment. As sensor nodes are deployed, the CHs will randomly assemble the common slices and send the series to sensors for rebuilding the KGFs for re-keying. The re-keying functions are rebuilt in each predefined interval, such that it would be difficult for an attacker to crack the functions in time. But this method did not prevent the CH comprised attack is appropriate only for static clustering schema. The author of [27] proposed an IDS based on GA for detecting the misbehaviors based on node attributes. However, this algorithm applied to multilayer network such as multi-hope clustering model but the author did not provide additional information about the network structure building process. Finally, a novel artificial immune system based random keying technique for clustered sensor network was proposed on [23]. This algorithm works well with dynamic clustering environment. But according to [22], this scheme performs well against the outsider attack in comparison to the insider attack.

### 5.16 Additional Methods

In [43], a secure clustering method was proposed based on multi-path route discovering. This method was proposed to deal with the malicious behaviors of the data aggregation nodes and the malicious route behaviors of the nodes in WSN.

In this method, the trusted value and residual energy for the nodes are used to choose the data aggregation nodes, a relatively reliable path is secretly selected to transfer the data aggregation results, and a secure clustering and reliable disjoint multi-path route discovery method is proposed by the functional-trust based secure data aggregation method. As general, this method represents an excellent solution for all types of passive attacks. It also provides a way to avoid the physical kinds of attacks like node destruction and node malfunction. On the other side, the efficiency is big challenge. A hybrid key management scheme for secure clustering in WSN was proposed at [44]. However, this method requires special characteristics for CH nodes. So, it works only with the heterogeneous clustering model in which nodes may differ in their features, i.e., processing power, memory size, initial energy, and transmission range.

## 6 SECURE CLUSTERING ALGORITHMS ANALYSIS AND EVALUATION

In this section, we provide a group evaluation of the dis- cussed secure clustering protocols based on security goals, various routing attacks, performance, and cluster building metrics based on the proposed criteria. To clarify and summarize the advantages and the limitations of the above methods according to completeness, efficiency, and dynamic clustering criteria, Table III is constructed. Also, Table IV provides the evaluation of these algorithms based on the robustness criteria and the security goals. Table IV also provides a list of attacks that each protocol prevents.

Based on Table III and Table IV, if we select the completeness as the only evaluation criteria, ORLEACH, SRPSN, SecRout, and the proposed algorithm in [43] are the most secure clustering algorithms. On the other side, the dynamic clustering criteria is applied by SLEACH, SecLEACH, RLEACH, ORLEACH, EECBKM, the proposed algorithm in [43], SHEER, AKM, SRPSN, SecRout, and IKDM algorithms. Where the efficiency criteria is applied by SecRout, AKM, and IKDM algorithms.

Related to the types of attacks, the work of most of the existing algorithms concentrated on preventing the CH attack in which an external malicious node tries to act as CH to collect data from the cluster members [8]. In addition, most of these procedures greatly decrease the network efficiency during the data aggregation process by using complicated cryptography schema. However, it seems that the algorithms that used cryptography and hashing together as the security mechanisms, i.e., ESODR and SecLEACH, are closer to the desired solution. Most of them provided a good solution for many kinds of both passive and active attack. We think that with searching about good solution for the key management problem, these algorithms may achieve the required balancing between security requirements and the network performance. Concerning to the security goals and robustness, we observe that AKM and IKDM secure clustering protocols maintain the most whereas SCMRP, RLEACH, and NSKM gain the least. We observe that SecLEACH, SHEER, EECBKM, AKM, and IKDM address all the security goals. According to the security goals, all the listed secure clustering algorithms applied integrity.

Finally, we can say most of secure clustering protocols for WSNs use the symmetric key schemes due to their less computation time compared with the other schemes. Any secure clustering algorithm for WSN must guarantee not only the four phases of secure clustering, but also all other criteria which we used to evaluate the existing algorithms. For example, in ORLEACH algorithm, the four phases are applied but the algorithm still requires high memory storage for each sensor, consumes more energy through its need for additional processing and computation time. So, we cannot apply security and ignore the network performance which affects its lifetime.

## 7 SUMMARY

Wireless Sensor Network (WSN) consists of set of sensor devices with limited resources and transpired in tangible insecure environments in order to collect data, which make security an essential challenge. For the sake of increasing the network lifetime and reducing the energy consumption, the cluster based model was proposed. In order to apply security for clustering model, many security procedures for the wireless sensor networks have been proposed. Most routing protocols are vulnerable to a number of security threats and are applied to the fixed clustering schema. Therefore, this paper is an attempt to comprehensively review and critically discuss the most prominent secure clustering routing algorithms that have been developed for WSNs. It explained the steps towards building a simple solution that allow securing the dynamic cluster network while consuming as little energy as possible and is adapted to a low computing power. We proposed four phased towards building a secure clustering algorithm for WSN. These phases are secure cluster head selection, secure cluster formation, secure data aggregation by the cluster head from its cluster nodes, and secure data routing to the base station. In order to build a secure clustering algorithm, this algorithm must guarantee not only the four phases of secure clustering, but also all criteria proposed in this paper, i.e., efficiency, robustness, and dynamic clustering.

## 8 REFERENCES

[1] S. Ganesh and R. Amutha. Efficient and secure routing protocol for wireless sensor networks through SNR based dynamic clustering mechanisms. Journal of Communications and Networks, 15(4):422–429, 2013.

[2] S. Soonhwa and R. Jaecheol. ID-based sensor node authentication for multi-layer sensor networks. Journal of Communications and Networks, 16(4):363– 370, 2014.

[3] J. Lotf, S. Hossein, and N. Ghazan. Overview on wireless sensor networks. Journal of Basic and Applied Scientific Research, 11(1):2811–2816, 2011.

[4] S. Sahraoui and S. Bouam. Secure routing optimization in hierarchical cluster-based wireless sensor networks. International Journal of Com- munication Networks and Information Security, 5(3), 2013.

[5] G. Padmavathi and D. Shanmugapriya. A survey of attacks and security mechanisms and challenges in wireless sensor networks. International Journal of Computer Science and Information Security, 4(1), 2009.

[6] I. Butun, S. Morgera, and R. Sankar. A survey of intrusion detection systems in wireless sensor networks. IEEE Communications Surveys and Tutorials, 16(1), 2014.

[7] N. Alrajeh, S. Khan, and B. Shams. Intrusion detection systems in wireless sensor networks: A review. International Journal of Distributed Sensor Networks, 2013.

[8] A. Diop, Y. Qi, Q. Wang, and S. Hussain. An advanced survey on secure energy efficient hierarchical routing protocols in wireless sensor networks. International Journal of Computer Science Issues, 10(1), 2013.

[9] S. Tyagia and N. Kumarb. A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks. Journal of Network and Computer Applications, 36(2):623–645, 2013.

[10] S. Sharma and S. Jena. A survey on secure hierarchical routing protocols in wireless sensor networks. In International Conference on Communication, Computing and Security, 2011.

[11] P. Schaffer, K. Farkas, A. HorvTh, T. Holczer, and L. ButtyN. Secure and reliable clustering in wireless sensor networks: A critical survey. The International Journal of Computer and Telecommunications Networking, 56(11):2726–2741, 2012.

[12] M. Rahayu, S. Lee, and H. Lee. Survey on LEACH based security pro- tocols. In 16th International Conference on Advanced Communication Technology, pages 304–309. IEEE, 2014.

[13] A. Bhattacharjee, B. Bhallamudi, and Z. Maqbool. Energy efficient hier- archical cluster based routing algorithm in WSN: a survey. International Journal of Engineering Research and Technology, 2(5):302–311, 2013.

[14] M. Rahayu, S. Lee, and H. Lee. Security analysis of secure data aggregation protocols in wireless sensor networks. In 16th International Conference on Advanced Communication Technology, pages 471– 474. IEEE, 2014.

[15] J. Guo, J. Fang, and X. Chen. Survey on secure data aggregation for wireless sensor networks. In IEEE International Conference on Service Operations and Logistics and Informatics, pages 138 –143. IEEE, 2011.

[16] J. Jose, J. Jose, and F. Jose. A survey on secure data aggregation pro- tocols in wireless sensor networks. International Journal of Computer Applications, 55(18):17–21, 2012.

[17] M. Patel and A. Aggarwal. Security attacks in wireless sensor networks: A survey. In International Conference on Intelligent Systems and Signal Processing, pages 329–333, 2013.

[18] A. Fuchsberger. Intrusion detection systems and intrusion prevention systems. Elsevier Journal Information Security, 10(3):134–139, 2005. [19] C. Dhivya Devi and B. Santhi. Study on security protocols in wireless sensor networks. International Journal of Engineering and Technology, 5(5):200–207, 2013.

[19] A. Semary and M. Abdel-Azim. New trends in secure routing protocols for wireless sensor networks. International Journal of Distributed Sensor Networks, 2013, 2013.

[20] M. Zhang, M. Kermani, A. Raghunathan, and N. Jha. Energy-efficient and secure sensor data transmission using encompression. In International Conference on VLSI Design and the 12th International Conference on Embedded Systems, 2013.

[21] M. Singh and M. Hussain. A top-down hierarchical multi-hop secure routing protocol for wireless sensor networks. International Journal of Ad hoc and Sensor and Ubiquitous Computing, 1(2), 2010.

[22] E. Sandeep, S. Kusuma, and B. Kumar. A random key distribution based artificial immune system for security in wireless sensor networks. In IEEE International Students' Conference on Electronics, Electrical and Computer Science, 2014.

[23] L. Oliveira, A. Ferreira, M. Vilaca, H. Wong, M. Bern, R. Dahab, and Loureiro. Secleach-on the security of clustered sensor networks. Signal Processing, 87(12):2882–2895, 2007.

[24] B. Shanthini and S. Swamynathan. Genetic-based biometric security system for wireless-sensor-based healthcare systems. In International Conference on Recent Advances in Computing and Software Systems, pages 180–184, 2012.

[25] K. Grgic, D. Zagar, and V. Krizanovic. Security in ipv6-based wire- less sensor network precision agriculture example. In International Conference on Telecommunications, pages 79–86, 2013.

[26] B. Radhika, P. Raja, C. Joseph, and M. Reji. Node attribute behavior based intrusion detection in sensor networks. International Journal of Engineering and Technology, 5(5):3692–3698, 2013.

[27] T. Lalitha and R. Umarani. Energy efficient cluster based key manage- ment technique for wireless sensor network. International Journal of Advances in Engineering and Technology, 3(2):186–190, 2012.

[28] N. Alrajeh, S. Khan, J. Lloret, and J. Loo. Secure routing protocol using cross layer design and energy harvesting in wireless sensor networks. International Journal of Distributed Sensor Networks, 2013, 2013.

[29] A. Salehi, M. Razzaque, P. Naraei, and A. Farrokhtala. Security in wireless sensor networks: Issues and challanges. In IEEE International Conference on Space Science and Communication, pages 356–360,2013.

[30] G. Wang, D. Kim, and G. Cho. A secure cluster formation scheme in wireless sensor networks. International Journal of Distributed Sensor Networks, 2012, 2012.

[31] H. Rifa-Pous and J. Herrera-Joancomart. A fair and secure cluster for- mation process for ad hoc networks. Wireless Personal Communications, 56(3):625–636, 2011.

[32] D. Wu, G. Hu, and G. Ni. Research and improve on secure routing protocols in wireless sensor networks. In Fourth IEEE International Conference on Circuits and Systems for Communications, pages 853– 856. IEEE, 2008.

[33] Y. Zhang and L. Xu. An efficient secure on-demand routing in clustered wireless ad hoc networks. In International Conference on Wireless Communications, Networking and Mobile Computing. IEEE, 2008.

[34] I. Gawdan, C. Chow, T. Zia, and Q. Sarhan. A novel secure key manage- ment for hierarchical wireless sensor network. In Third Conference on Computational Intelligence, Modeling and Simulation, pages 312–316. IEEE, 2011.

[35] S. Kumar and S. Jena. SCMRP: secure cluster based multipath routing protocol for wireless sensor networks. In Sixth International Conference on Wireless Communication and Sensor Networks, pages 1–6. IEEE, 2010.

[36] J. Ibriq and I. Mahgoub. A secure hierarchical routing protocol for wireless sensor networks. In IEEE International Conference on Communication Systems, pages 1–6. IEEE, 2006.

[37] F. Kausar, A. Masood, and S. Hussain. An authenticated key man- agement scheme for hierarchical wireless sensor work. Advances in Communication Systems and Electrical Engineering, 4:85–98, 2008.

[38] M. Tubaishat, J. Yin, B. Panja, and S. Madria. A secure hierarchical model for sensor network. ACM Sigmod Record, 33(1):7–13, 2004.

[39] J. Yin and S. Madria. Secrout a secure routing protocol for sensor network. In IEEE International Conference on Advanced information networking and applications, volume 1, 2006.

[40] Y. Cheng and D. Agrawal. An improved key distribution mechanism for large scale hierarchical wireless sensor networks. Ad Hoc Networks, 5(1):35–48, 2007.

[41] C. Wang, T. Hong, G. Hoing, and W. Wang. A ga- based key- manage- ment scheme in hierarchical wireless sensor networks. International Journal of Innovative Computing, Information and Control, 5:4693– 4702, 2009.

[42] C. Zhong, M. Yinghong, J. Zhao, C. Lin, and X. Lu. Secure clustering and reliable multipath route discovering in wireless sensor networks. In Sixth International Symposium on Parallel Architectures and Algorithms and Programming, pages 130–134. IEEE, 2014.

[43] P. Zhao, Y. Xu, and M. Nan. A hybrid key management scheme based on clustered wireless sensor networks. Wireless Sensor Network, 4:197– 201, 2012.

*Table 3: Secure Clustering Protocols Analysis According to Completeness, Efficiency, and Dynamic Clustering Criteria*

| Algorithm | Mechanism | Completeness | | | | Efficiency | | | Dynamic Clustering | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | S-CH | S-CF | S-DA | S-DR | M | E | P | D | S |
| SLEACH | Cryptography | √ | √ | ✗ | ✗ | High | Low | Medium | √ | √ |
| ESODR | Cryptography+ | √ | √ | ✗ | √ | High | Low | Low | ✗ | √ |
| SecLEACH | Cryptography + | √ | ✗ | √ | √ | High | Low | Low | √ | √ |
| RLEACH | Cryptography | √ | √ | √ | ✗ | Medium | Low | Medium | √ | √ |
| ORLEACH | IDS+ Cryptography | √ | √ | √ | √ | High | High | Low | √ | √ |
| EECBKM | Cryptography | √ | √ | ✗ | ✗ | Low | Low | Low | √ | √ |
| [42] | Cryptography | ✗ | √ | √ | √ | Medium | Medium | Low | ✗ | √ |
| [27] | IDS | - | - | - | - | Low | High | Medium | - | - |
| [23] | Cryptography | √ | √ | ✗ | √ | Medium | Medium | Medium | √ | √ |
| NSKM | Cryptography | √ | √ | √ | ✗ | Low | Medium | High | ✗ | √ |
| SS-LEACH | Multi-path | √ | √ | ✗ | ✗ | High | Medium | High | ✗ | √ |
| [43] | Multi-path | √ | √ | √ | √ | Low | Medium | Medium | √ | √ |
| SCMRP | Multi-path | √ | √ | √ | √ | Medium | Medium | High | ✗ | √ |
| [44] | Cryptography | √ | √ | √ | ✗ | High | High | Medium | √ | √ |
| SHEER | Cryptography | √ | √ | ✗ | √ | Low | Low | Medium | √ | √ |
| AKM | Cryptography | √ | √ | √ | ✗ | Low | Low | High | √ | √ |
| SRPSN | Cryptography | √ | √ | √ | √ | Medium | Medium | Medium | √ | √ |
| SecRout | Cryptography | √ | √ | √ | √ | Low | Low | High | √ | √ |
| IKDM | Cryptography | √ | ✗ | √ | √ | Low | Low | High | √ | √ |

*Table 4: Secure Clustering Protocols with Security Goals and Robustness Criteria*

| Algorithm | Integrity | Confidentiality | Availability | Freshness | Prevents Attacks |
|---|---|---|---|---|---|
| SLEACH | √ | ✗ | √ | √ | A2, A3, A6, A7, A11, A14 |
| ESODR | √ | √ | √ | ✗ | A2, A3, A4, A6, A10, A11, A14 |
| SecLEACH | √ | √ | √ | √ | A2, A4, A6, A7, A11 |
| RLEACH | √ | ✗ | ✗ | √ | A2, A3, A4, A6, A11, A14 |
| ORLEACH | √ | √ | √ | ✗ | A1, A2, A3, A4, A6, A9 |
| EECBKM | √ | √ | √ | √ | A3, A4, A6, A12 |
| [42] | √ | ✗ | √ | ✗ | A2, A3, A4, A5, A6, A15 |
| [27] | √ | √ | ✗ | √ | A1,A2, A6, A7, A8, A11, A14 |
| [23] | √ | ✗ | ✗ | √ | A2, A3, A4, A6, A7, A10, A12 |
| NSKM | √ | ✗ | √ | √ | A2, A3, A4, A5, A6, A15 |
| SS-LEACH | √ | ✗ | √ | ✗ | A2, A4, A6, A7, A9, A11, A12 |
| [43] | √ | √ | √ | ✗ | A1, A2, A9, A11, A12, A14, A15 |
| SCMRP | √ | √ | ✗ | ✗ | A2, A3, A5, A6, A7, A13 |
| [44] | √ | ✗ | √ | ✗ | A2, A5, A6, A7, A11, A13, A14 |
| SHEER | √ | √ | √ | √ | A3, A4, A5, A6, A9, A14, A15 |
| AKM | √ | √ | √ | √ | A2, A4, A5, A6, A7, A14 |
| SRPSN | √ | ✗ | √ | √ | A1, A2, A5, A6, A9, A11, A13 |
| SecRout | √ | ✗ | √ | √ | A2, A5, A6, A8, A9, A10, A13, |
| IKDM | √ | √ | √ | √ | A2, A3, A4, A6, A9 ,A11, A14 |