International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT2176108

A Survey on Attacks, Security Mechanisms and Secure Extensions of Hierarchical Clustering Based Sensor Networks

Saziya Tabbassum, Sanjeev Bangarh
Department of Computer Science, OPJS University Churu, Rajasthan, India

Article Info
Volume 8, Issue 1
Page Number : 05-24

Publication Issue :
January-February-2022

Article History
Accepted : 01 Jan 2022
Published : 04 Jan 2022

ABSTRACT

Wireless Sensor Networks (WSNs) consists of large number of sensors deployed in regions required by the applications to collect information about the surrounding environment. WSNs are highly vulnerable to security attacks at various levels due to their distributed nature, multi-hop data forwarding, and open wireless medium. A clustering-based routing protocol LEACH is a successful protocol for routing in WSNs as well as evenly utilizing energy of sensor nodes since all sensor nodes have limited source of energy. However, LEACH protocol also has some flaws which can attract attackers and they can cause serious damage either physically or it can also steal information from the network. Due to this reason security is the main problem of LEACH protocol and many secure versions of this protocol have been designed to make it resilient against insider as well as outsider attackers. In this paper, we discuss some of the threats in WSNs along with various kinds of attacks as well as mechanism to deal with such threats. Furthermore, we discuss LEACH protocol and its extensions, various techniques used to define secure LEACH which can protect network from entering intruders. Lastly, we compare some secure LEACH schemes like cryptographic-based or trust-based scheme.

Keywords : Wireless Sensor Network, LEACH, Attacks, Security Threats, Security Mechanism, Secure LEACH

I. INTRODUCTION

Sensors are used to monitor the physical or environmental conditions in Wireless Sensor Network (WSN) where, wireless network consists of spatially distributed autonomous device deployed in the required region. To find out characteristics of the phenomenon located in the area around these sensors, they measure conditions in the environment surrounding them and then transform these measurements into signals which can be processed. Once these signals are processed then the signal is transferred from these sensor nodes to the base station through the gateway where the distance between the place where sensor nodes are deployed and base station depends on application of the network. These measured data from sensor nodes either can go directly to the base station (BS) or it can

choose certain multiple hops to reach the BS. In multiple hops mode nodes transmit the sensed data to the sink via relay nodes and from sink to the BS [1-5]. With recent technological advances in micro-electro mechanical systems (MEMS), [6] wireless communication and digital electronics have proved low-cost, low-power, multi-functional sensors with capabilities of sensing, data processing and wireless communication within short range. The intrinsic properties of individual sensor nodes pose additional challenges to the communication protocols in terms of energy consumption. These sensor nodes consist of a sensing, communication, processing, power unit which helps to execute all the functionality of the sensor nodes. Location information can easily be provided by GPS, which provides accuracy up to 10m through the recent GPS unit developed for WSNs. However, the cost of these units is significantly higher than a single sensor node so instead, a limited number of nodes, which use GPS or other means to identify their location, are used to help the other nodes determine their locations. Due to the short transmission ranges, large numbers of sensor nodes are densely deployed and neighbouring nodes may be very close to each other. But for far transmission more power is required which leads to dead sensor nodes very early. Hence, multi-hop communication is used in communications between nodes since it leads to less power consumption than the traditional single-hop communication. Once these sensor nodes are deployed it becomes almost impossible to replace or recharge their batteries, they have limited power, sensing, computation and wireless communication capabilities. So, to solve this problem, solution is to deploy a large number of sensor nodes in the required area. Based on the structure of the network, routing protocols are classified as flat-based routing, hierarchical routing and location-based routing.

Flat-based routing also known as data-centric routing is a multi-hop routing protocol in which each node plays the same role and sensor nodes collaborate to perform the sensing task. The BS sends queries to certain regions and wait for data from the sensors located in the selected regions. Some of the routing protocols are Sensor Protocols for Information via Negotiation (SPIN) [7,8], Directed Diffusion [9], Rumour Routing [10], Gradient-Based Routing [11].

Hierarchical routing also known as cluster-based routing methods is utilized to perform energy-efficient routing in WSNs. In a hierarchical architecture, higher-energy nodes can be used to process and send the information, while low-energy nodes can be used to perform the sensing in the proximity of the target. The creation of clusters and assigning special tasks to cluster heads can greatly contribute to overall system scalability, lifetime, and energy efficiency. Hierarchical routing is an efficient way to lower energy consumption within a cluster, performing data aggregation and fusion in order to decrease the number of transmitted messages to the BS. Hierarchical routing is mainly two-layer routing where one layer is used to select cluster heads and the other for routing. Routing protocols in this structure are Low Energy Adaptive Clustering Hierarchy (LEACH) [5], Power-Efficient Gathering in Sensor Information Systems (PEGASIS) [12], Threshold-Sensitive Energy Efficient Network Protocol (TEEN) [13], Adaptive Periodic TEEN (APTEEN) [14], Virtual Grid Architecture Routing [15].

In location-based routing sensor nodes are addressed by means of their locations. The distance between neighbouring nodes can be estimated on the basis of incoming signal strengths. Relative coordinates of neighbouring nodes can be obtained by exchanging such information between neighbours [1, 2, 16]. Alternatively, the location of nodes may be available directly by communicating with a satellite using GPS if nodes are equipped with a small low-power GPS receiver [17]. To save energy, some location-based schemes demand that nodes should go to sleep if there is no activity. More energy savings can be obtained by having as many sleeping nodes in the network as

possible. The problem of designing sleep period schedules for each node in a localized manner was addressed in [17,18]. Some of the routing protocols in this structure are Geographic Adaptive Fidelity (GAF) [17], Geographic and Energy Aware Routing (GEAR) [19], Most Forward within Radius (MFR), Distance Routing (DIR), Geographic Distance Routing (GEDIR) [20], SPAN [18].

With all these advancements there comes some security related threats which may compromise the privacy of data, resources, network structure, and many more. There exist various kinds of threats which can modify or drop the information that is being transmitted to the BS from sensor nodes. In this paper we are going to study various threats on sensor network, one of the clustering protocols- LEACH, and its secure extensions. Our work is a dedicated study of basically security related threats in WSNs, and mechanisms to deal with such attacks along with it we have studied security mechanisms in LEACH protocol.

II. GOALS OF SECURITY IN SENSOR NETWORK

In WSNs, security is the degree of protection to safeguard network, sensors and their transmitted data against various attackers and malicious nodes. Mainly, security deals with providing following services in the network:

A. Data Confidentiality

It is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. It ensures that sensed and transmitted information is never revealed to unauthorized nodes. Data privacy can be achieved in hop-by-hop or end- to-end basis.

B. Data Authentication

This property ensures the reliability of the message by identifying its origin. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject additional false packets [11]. In data authentication identification of the senders and receivers are done which can be achieved through symmetric or asymmetric mechanisms were sending and receiving nodes share secret keys. Because of the wireless nature of the media and the unattended nature of sensor networks, it is extremely challenging to ensure authentication.

C. Data Integrity

In sensor network data integrity is required to ensure the reliability of the data and refers to the ability to confirm that a message has not been tampered, altered or changed. Whenever, a malicious node is present in the network and try to inject false data or unstable conditions due to wireless channel cause damage or loss of data then the integrity of the network will be in trouble.

D. Data Availability

It ensured that services offered by WSN or a single sensor node must be available whenever required, i.e., node has the ability to use the resources and network is available for the messages to communicate. Some schemes achieve this property by the use of multipath routing and others use self-healing to diagnose and react.

E. Data Freshness

There is a need to ensure the freshness of each message even if there is assurance of data confidentiality and data integrity. Data freshness means that the data is recent, and it ensures that no old message have been replayed. Sometime related counter can be added into the packet to ensure data freshness.

III. ATTACKS IN SENSOR NETWORK

WSNs are vulnerable to various security threats due to the broadcast nature of the transmission medium and also because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Due to the unique characteristics like wireless medium, decentralized architecture, random deployment, multi-hop nature these networks make

them more vulnerable to security attacks at various layers. There exist two types of attackers outside attackers and insider attackers in which outsider attackers has no special access to the sensor network. But in case of insider attackers, an authorized participant in the sensor network has gone bad. It may be mounted from either compromised sensor nodes running malicious code or adversaries who have stolen the key material, code, and data from legitimate nodes

Attacks are basically classified as active attacks and passive attacks. Active attacks are unauthorized attackers which monitors, listens to and modify data stream in the communication channel. In other words, active attacks are used to misdirect, temper, or drop packets. Various active attacks are as follows:

A. Routing Attacks in Sensor Networks

Routing attacks generally occurs in network layer and happens generally while routing the message. Spoofed, altered or replayed routing information, selective forwarding, sinkhole attack, sybil attack, wormhole attacks, HELLO flood attack are some of the routing attacks in sensor network [22].

1) ***Spoofed, Altered or Replayed Routing Information:*** as each node in the network acts as a router, and directly affects the routing information by creating routing loops, extend or shorten service routes, generates false error message and increase end-to-end latency.
2) ***Selective Forwarding:*** in WSNs it is assumed that whenever a node receives a message it forwards that message. But if there exists compromised node in a network, it might refuse to forward packet and its neighbouring node might use another route. A malicious node can selectively drop only certain packet in selective forwarding type of attack.
3) ***Sinkhole Attack:*** in this attack, the main goal is to attracting traffic to a specific node i.e., to attract nearly all the traffic from a particular area through a compromised node. This attack has a tendency to make a compromised node look especially attractive to surrounding nodes. Since all packets share the same ultimate destination i.e., in networks with only one base station, a compromised node needs only to provide a single high-quality route to the base station in order to influence a potentially large number of nodes.
4) ***Sybil Attack:*** in this attack, a single node duplicates itself and presented in the multiple locations. The Sybil attack targets fault tolerant schemes such as distributed storage, multipath routing and topology maintenance. In a Sybil attack, a single node presents multiple identities to other nodes in the network. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network.
5) ***Wormhole Attack:*** in a wormhole attack attacker receives a message in one part of the network, tunnels it over a low-latency link and replay that message to different part of the network. A compromised node could convince nodes which are multiple hops from a base station that they are just one or two hops away via the wormhole thus, creating a sinkhole. Wormhole attacks would likely be used in combination with selective forwarding or eavesdropping.
6) ***HELLO Flood Attack:*** in HELLO flood attack an attacker sends or replays a routing protocol HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes that are isolated in a large area within a WSN. The sensors are thus influenced that the adversary is their neighbour. As a result, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it

is their neighbour and are ultimately spoofed by the attacker.

B. Denial of Service Attack

The unintentional failure of nodes or malicious actions produces Denial of Service (DoS) attack. This attack not only attempts to disrupt, or destroy a network but also for any event that diminishes a networks capability to provide a service. In WSNs there are several types of DoS attacks in different layers like at physical layer the it is jamming and tampering, at the link layer, collision, exhaustion and unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization. Payment for network resources, pushback, strong authentication and identification of traffic are few mechanisms to prevent DoS attacks.

C. Physical Attack

Sensor networks generally works in outdoor hostile environment where, they are unattended and distributed nature of their deployment. Because of this reason they are highly susceptible to physical attacks, i.e., threats due to physical node destructions. Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker.

D. Node Replication Attack

In a node replication attack, an attacker seeks to add a node by copying the node ID of an existing sensor node to an existing sensor network resulting in severely disrupting the sensor networks performance, packets can be corrupted or even misrouted. This can be followed by disconnected network, false sensor readings, etc. If an attacker can gain physical access to the entire network, he can copy cryptographic keys to the replicated sensor nodes. By inserting the replicated nodes at specific network points, the attacker could easily manipulate a specific segment of the network, perhaps by disconnecting it altogether.

In passive attacks, monitoring and listening of the communication channel by unauthorized attackers are done. Since sensor network makes large volumes of information easily available through remote access therefore the privacy problem is intensified. Hence, adversaries need not be physically present to maintain surveillance. They can gather information at low-risk in anonymous manner. The attacks against privacy are passive in nature where monitor and eavesdropping, traffic analysis, camouflage adversaries are some of the passive attacks.

E. Monitor and Eavesdropping

Communication contents can be easily discovered by the attackers by snooping to the data. The eavesdropping acts effectively against the privacy protection, when the traffic conveys the control information about the sensor network configuration, which contains potentially more detailed information than accessible through the location server.

F. Traffic Analysis

There exists high possibility analysis of communication pattern even if the messages which are being transferred are encrypted. To enable an attacker to cause malicious harm to the sensor network sensor activities reveal enough information.

G. Camouflage Adversaries

To hide in the network the attackers can insert a node or compromise the nodes. Once this is done then these nodes can copy as a normal node to attract the packets, then change the route of packets and finally conducting the privacy analysis.

IV. SECURITY MECHANISM

WSNs are vulnerable to various level of threats as we have seen in last section. It can harm the network or

the data which are being collected in that network by many ways. To detect, prevent and recover from security attacks security mechanisms are used. A wide variety of security mechanisms can be invented to counter these malicious attacks and some of which can be categorised as high and low level of security mechanisms.

A. High-Level Mechanisms

In a high-level category secure group management, intrusion detection and secure data aggregations are some of the mechanisms [23].

1) ***Secure Group Management***: in WSN every node has limited computing and communication capabilities. But for data aggregation and analysis of data groups of nodes are involved. So, secure protocols for group management are required for securely admitting new group members and supporting secure group communication. For example, key services in WSN are performed by groups, vehicle tracking using network requires a group of nodes to work jointly. The group key once computed it should be authenticated to ensure that it comes from a valid group and later its outcome should be transmitted to a base station.
2) ***Intrusion Detection:*** Any sort of unlawful activity which is carried out by an attacker to harm network resources or sensor nodes are called intrusion. Intrusion detection is a mechanism to detect such unlawful or malicious activity. The primary functions of intrusion detection are to monitor user activities and network behaviour at various layers. WSNs require a solution that is fully distributed and inexpensive in terms of communication, energy, and memory requirements. The use of secure groups may be a promising approach for decentralized intrusion detection.
3) ***Secure Data Aggregation:*** WSNs are full of fine grain sensing provided by large and dense sets of nodes. To avoid the overwhelming amounts of traffic back to the base station the sensed value must be aggregated. Based on the architecture of WSN aggregation may take place in many places in the network and all the aggregation location must be secured. For example, the system may average the temperature of a geographic region, combine sensor values to compute the location and velocity of a moving object, or aggregate data to avoid false alarms in real-world event detection [24].

B. Low-Level Mechanisms

Key Establishment and Trust Setup, Secrecy and Authentication, Privacy, Robustness to communication, denial of service, Secure Routing, Resilience to Node Capture are some of the low-level security mechanisms.

A. ***Key Establishment and Trust Setup:*** the sensor nodes have very limited energy source and public key cryptography primitives are too expensive. To secure the network establishment of cryptographic key is the primary requirement. This key establishment technique should be scaled to hundreds or thousands of nodes in the network. The sensor nodes need to setup keys with their neighbours and with data aggregation nodes as the communication patterns of sensor networks differ from traditional networks [23].

B. ***Secrecy and Authentication:*** Cryptography is the standard defence and whenever we incorporate cryptography into sensor networks a remarkable system trade-off arises. Sensor network applications require protection against eavesdropping, injection, and modification of packets. A high level of security is achieved by end-to-end cryptography for point-to-point communication but for that it requires that keys be setup among all end points and be incompatible with passive participation and local broadcast. Link-layer cryptography with a

network wide shared key simplifies key setup and supports passive participation and local broadcast, but intermediate nodes might eavesdrop or alter messages. The earliest sensor networks are likely to use link layer cryptography, because this approach provides the greatest ease of deployment among currently available network cryptographic approaches [24].

C. ***Privacy:*** the sensor networks are deployed initially for legitimate purpose which might subsequently use in unanticipated ways. Like other traditional networks, the sensor networks have also force privacy concerns. Providing awareness of the presence of sensor nodes and data acquisition is particularly important [23].

D. ***Robustness to communication denial of service:*** by broadcasting a high-energy signal an attacker can attempt to disrupt the network operation. The entire systems communication could be jammed if the transmission is powerful enough. More sophisticated attacks are also possible; the attacker might inhibit communication by violating the 802.11 medium access control (MAC) protocol by, say, transmitting while a neighbour is also transmitting or by continuously requesting channel access with a request-to-send signal [23].

E. ***Secure Routing:*** Recent routing protocols suffer from many security vulnerabilities and enabling communication in sensor networks is very crucial service by routing and data forwarding. For example, an attacker might launch denial of service attacks on the routing protocol, preventing communication. The simplest attacks involve injecting malicious routing information into the network, resulting in routing inconsistencies. Simple authentication might guard against injection attacks, but some routing protocols are susceptible to replay by the attacker of legitimate routing messages [24].

F. ***Resilience to Node Capture:*** in WSN, sensor nodes are deployed randomly based on the requirement of the applications in hostile environment which are easily accessible by the attackers. Such exposure raises the possibility that an attacker might capture sensor nodes, extract cryptographic secrets, modify their programming, or replace them with malicious nodes under the control of the attacker. Tamper-resistant packaging may be one defence, but it is expensive, since current technology does not provide a high level of security. So, another solution is algorithmic solutions to the problem of node capture is preferable [23].

V. LEACH

Heinzelman and et al [5] develop communication protocols which can have a significant impact on the overall energy dissipation of the networks. LEACH (Low Energy Adaptive Clustering Hierarchy), which is a cluster-based protocol for data transmission from the environment to the base station. The operations of LEACH are divided into a number of rounds and each round consists of two phases: set-up phase, in which clustering is done and the steady state phase, in which data is being sent to the base station from all the sensors. Initially, when the clusters are formed in the set-up phase all sensor nodes decide to become a cluster head (CH) or not in the current round. This decision is made by node n, choosing a random number between 0 and 1. If the number is less than threshold value $T(n)$, then it becomes a cluster head (CH) for the current round where $T(n)$ is given by

$$T(n) = \begin{cases} \frac{P}{1-P*(r \bmod \frac{1}{P})}, & if\ n \in G \\ 0, & otherwise \end{cases} \quad (1)$$

Where, P is the desired percentage of cluster head, r is the current round and G is the set of nodes that have not been cluster head in the last $\frac{1}{P}$ round.

Now the nodes elected as CH broadcast advertisement message done by CSMA MAC protocol which is

received by the non-CH nodes. The non-CH decides to which CH they should join according to the signal strength of received advertisement message. Once the nodes decide to which CH they belong, they inform the CH node that it will be member of the cluster by transmitting information back to CH using CSMA MAC protocol. After getting the information of the cluster members the CH broadcast TDMA schedule back to nodes telling each node when it can transmit. When the clusters are formed and TDMA schedule is fixed then only data transmission can be done and hence there comes steady state phase. The nodes in each cluster then transmit data to the CH of that cluster in the allocated time slot. Now CH has lots of similar types of data collected from many nodes in the cluster then, it performs signal processing function to compress the data into a single signal. This signal is then sent to the base station which is far away and requires a high energy transmission. After a certain time, the next round begins and the same procedure of the set-up phase and steady state phase is executed.

LEACH protocol reduces energy dissipation because of the following reason: reducing the number of transmissions to sink by using cluster heads. By aggregating the data at the cluster head data is compressed it reduces the data to transmit. Randomized rotation being as a cluster head increases the lifetime of the network. Nodes die randomly and dynamic clustering enhance network lifetime. It allows member nodes to remain in sleeping mode except for specific time duration. LEACH protocol has many descendants, few of them are LEACH-C, LEACH-F, LEACH-B, LEACH-E, LEACH-M, TL-LEACH, MH-LEACH, LEACH-A, etc.

Siva D. Muruganathan and et al in [3] have proposed a centralized routing protocol called Base-Station Controlled Dynamic Clustering Protocol (BCDCP) also known as LEACH-C, which distributes the energy dissipation evenly among all sensor nodes to improve network lifetime and average energy savings. In LEACH-C the number of CHs in each round is equal to a predetermined optimal value and computational tasks like a cluster set up, CH selection, routing path formation, and TDMA schedule creation is done by using base station [4]. The author shows that BCDCP outperforms its comparatives by uniformly placing CHs throughout the whole sensor field, performing balanced clustering, and using a CH-to-CH routing scheme to transfer fused data to the base station and also it provides an energy efficient routing scheme suitable for a vast range of sensing applications. Whereas, authors in [25] propose advance low energy adaptive clustering hierarchy (ALEACH) where nodes make autonomous decisions without any central intervention. Here, a new cluster head selection algorithm is proposed that enables selecting best suited node for cluster head, algorithms for adaptive clusters and rotating cluster head positions to evenly distribute the energy load among all the nodes. Since, the authors here select the most eligible nodes as the cluster-heads in terms of its current state and general probability, so the nodes death rate is less than the other compared protocols. Hence, in case data message reception at the base station and energy loss of the nodes it creates a great impact.

Dogar and et al [26] have proposed a protocol called multi-hop routing in which network is partitioned into various layers of clusters. Normal sensor nodes join CH based on received signal strength indicator (RSSI) whereas, CHs collaborate with the neighbor layer to transmit sensors data to base station. The base station controls the transmission of nodes which defines the TDMA schedule for CH. The base station selects upper layer CH to act as super CH for lower layer CHs. This protocol works on three phases: cluster formation at the lowest level, cluster discovery at different levels by the base station and, scheduling. The author has compared this protocol with a direct communication protocol and LEACH. Using direct communication protocol, the battery of nodes drains

out quickly resulting in reduction of network lifetime. It works on equal clustering and performance evaluation has shown that this protocol performs well as compared to similar approach given that network is divided into an optimal number of layers. Simple sensing nodes will join the CH afterward, the base station will choose the CHs for lower layer CH from its immediate upper layer CH. In this way clustering hierarchy will be formed till we reach the base station. There is another protocol called fixed-LEACH (LEACH-F), that uses centralized approach for cluster formation [27]. Once, it is done, then there is no re-clustering phase in next round. The cluster is fixed and only the rotation of CH node within its clusters. Here, overhead of clustering is removed, after the nodes are deployed and clusters are formed it remains as it is throughout the network lifetime. The main limitations of this approach are that it provides no flexibility of adding or removing the nodes once clusters are formed and nodes cannot adjust their behaviour on node dying.

Weichao and et al, introduced the concept of Trust, design the CH adjusting procedure and, establishes multipath with CHs acting as routers [17]. The author has introduced a variant of LEACH, LEACH-TM which adds CH adjusting procedure which enhances the robustness of the network by equilibrating the distribution of CHs. The result shows that LEACH-TM has evener cluster distribution and its lifetime is 4.81% longer than LEACH when network load is same. Here, authors have pointed three main advantages of their work compared with LEACH protocol as the introduction of trust and active trust transmission mechanism which provides an index for using network efficiently and safely. The number of CHs is much stable than that of LEACH and distribution of CH is evener. This protocol enables the path to avoid some suspected nodes and data load is also less than LEACH. While establishing node remaining energy, hop count, and node trust will enhance the transmission reliability to a certain extent.

The authors Minghao Tang and Mu Tong [28] have shown that at each round, after first selection of CH according to LEACH protocol, a second selection is done to modify the number of CH in consideration of nodes residual energy. As a result of this, the number of CH is constant and near optimal per round. In their work, authors have overcome the shortcomings of original protocol by taking the nodes residual energy and keeping the constant and near optimal number of CH at each round. In order to save the energy of consumption and prolong the network lifetime, the protocol needs to ensure that the partition of the cluster is balanced and uniform. Authors have analyzed that in their work a constant number of clusters and a balanced number of cluster distribution is done, so energy dissipation is balanced and near minimal in contrast to the huge fluctuation in LEACH protocol.

VI. SECURITY TECHNIQUES

LEACH is a clustering protocol based on hierarchical routing which operates in many rounds until all the sensor nodes are not dead. In each round there exist two phases: Setup Phase and Steady State Phase. In setup phase nodes are being deployed, clusters are formed and while these things are going and if there is no security mechanism then a malicious node may declare itself as a CH by broadcasting advertisement message. Attackers may join clusters in cluster setup phase or prevent some node to join the network. Attackers may achieve information about the cluster members and CH from clustering process. Attackers may try to disrupt the clustering process by DoS or jamming attacks. An attacker wants to make the CH have a false member list and create a wrong TDMA schedule [29]. To prevent from launching such attacks, security services such as authentication, integrity and freshness checking mechanism should be added to the

LEACH subphases. Also, Trust-based variants of LEACH prevent these attacks by using reputation management methods which rely on the history of nodes before actions. For providing more security, hybrid trust-based LEACH schemes apply both cryptographic and trust management methods to protect LEACH against internal and external attackers.

In steady state phase data are being collected from sensor nodes, it is being aggregated at the CHs of each clusters and finally send it to the BS. During this phase passive attackers may eavesdrop to transmitted data between cluster members and CH or traffic between CH and BS. Active attackers may use the time slots of an idle sensor node or they may send false data to sink node, on behalf of the idle sensor node or they may send false data on behalf of some CH to the BS. Attackers may try to disrupt the communication between the CHs and sink or CH and sensors by launching DoS or jamming attacks. To prevent the security problem of steady state phase CHs should authenticate its members before receiving data from them. BS should authenticate CHs before. Privacy, integrity and freshness of data transfer between CHs and its members and CHs and BS should be guaranteed. In addition to these properties ideally every mechanism for securing LEACH should consider the issues [30] for example, energy efficiency, isolation of malicious nodes, low number of node engagement, resistance to collusion attack, delay tolerance. Although having these properties in a secure clustering scheme, they are not enough for a complete secure system because even the best algorithms may produce incorrect results when applied incorrectly. The secure clustering schemes in WSN try to increase the security attributes of clustering algorithms and prevent the malicious behaviours to disrupt cluster creation and maintenance process. Almost all of the secure extensions of LEACH try to maintain its general structure and only add security features to existing phases of LEACH. In all of these schemes the basic security services such as data confidentiality, integrity and authenticity can be achieved by the deployment of cryptographic mechanisms. Here, we are going to discuss some of the security techniques to provide more reliable and attack resilient versions of LEACH and further few secure extensions of LEACH protocol.

A. Key Management Issue

Key management is a set of techniques that supports the establishment and maintenance of keys between authorized parties. The method of key management tells the security and scalability of encryption technique [29]. It can be classified as: self-enforcing schemes, arbitrated keying schemes and pre-distribution schemes. In Self-Enforcing Schemes asymmetric cryptography is used to establish keys after node deployment. Performance and high energy consumptions are the main drawback of this scheme which makes it inappropriate for WSNs. The Arbitrated Keying Schemes depends on a trusted central point for key management which becomes a preferred target for attacks. But in case of pre-distribution scheme a Key Distribution Centre (KDC) is responsible for loading keys into the sensors. After the deployment of nodes there is very little or no dependence on central station.

The Pre-Distribution Schemes has three keying models as network keying model, pairwise key and group keying schemes. The network keying scheme is simple and easy to use with highest scalability and flexibility. This scheme has lower resource consumption but it is most vulnerable to node capture. In network keying scheme it is easy to insert malicious nodes into the network and difficult to revocation of such nodes. The pairwise keying scheme has the highest security, resilience against node capture but low at scalability. The drawback of this scheme is the overhead of maintaining *N-1* unique key in each sensor node. The total number of *N(N-1)/2* distinguishable keys will be stored in network and due to this issue, the scalability is decreased [31]. But the Group Keying Scheme has the

combined features of both network and pairwise keying schemes. A single shared key is used within each group and a different key between each pair of groups. When one of the nodes is compromised, only the group key will be compromised and this will be less catastrophic. Scalability of this scheme is higher than pairwise method, because the number of keys increases with the number of groups, not with the size of the WSN. However, this scheme is difficult to set up and the formation of groups is a very application dependent.

B. One-Way Key Chain

Generation of a one-way key chain *{K0, K1, …, KR}* is done by iteratively performing the one-way hash function *H* on the last key in the chain. In key chain, the derivation of all former key chain can be obtained by computing $Ki = Hj - i(Kj)$, $0 \leq i < j$, while none of the later keys can be computed due to the one-wayness of the hash function. Therefore, with the knowledge of *K0 = H(K1),* anybody can verify the authenticity of any later key by only performing hash operations. The reason is that the attacker cannot change any hash value because the hash function in use is collision resistant.

C. Broadcast Authentication

Based on the communication pattern in LEACH, there exists two types of authentication: the first type is authenticated broadcast for broadcast from CHs and BS to rest of the network. Second type is pairwise authentication for node to CH and CH to BS communication. The two main methods for broadcast authentication that are used in secure LEACH scheme are μTESLA and LEAP. In μTESLA the receiver uses a one-way key chain to authenticate the broadcast message, they first authenticate the closed keys. The sender selects a random value K_n as the last key in the key chain and repeatedly performs a pseudo random function *F* to compute all the other keys: $K_i = F(K_{i+1})$, $0 \leq i \leq n-1$ where the secret key K_i is assigned to the i^{th} time interval. With the pseudo random function F, given K_j in the key chain, anybody can compute all the previous keys K_i, $0 \leq i \leq j$, but nobody can compute any of the later keys K_i, $j+1 \leq i \leq n$. Thus, with the knowledge of the initial key K_0, which is called the commitment of the key chain, a receiver can authenticate any key in the key chain by merely performing pseudo random function operations. When a broadcast message is available in i^{th} time interval, the sender generates MAC for this message with a key derived from K_i and then broadcasts this message along with its MAC and discloses the key K_{i-d} assigned to the time interval I_{i-d}, where *d* is the disclosure lag of the authentication keys. μTESLA uses a security condition to prevent a receiver from accepting any broadcast packet authenticated with a disclosed key.

LEAP it is a key management protocol known as Localized Encryption and Authentication Protocol [33], which supports the establishment of four types of keys for each sensor nodes: firstly, an individual key shared with the BS. The individual key Kmu = fKms (u), where f is a pseudo-random function and Kms is a master key. Secondly, a pairwise key shared with each of its immediate neighbour. Thirdly, a cluster key shared with all its neighbour and it is mainly used for securing locally broadcast message. And finally, a group key is shared by all the nodes in the network and is used by the BS for encrypting messages that are broadcast to the whole group. LEAP uses one-way hash key chain for one-hop broadcast authentication and does not use delayed key disclosure and time synchronization between neighbouring nodes.

D. Trust Management in WSNs

Cryptographic based LEACH provides some degree of protection against the external attackers, but they are unable to handle the internal threats and compromised sensors. Since these nodes already have the authentication keys and privileges that are required for passing the authentication processes and conventional authentication schemes are not been

able to detect it. Trust management systems overcome the shortcomings of cryptography-based approach and prevents these kinds of attacks. This can be achieved by collecting, distributing and aggregating feedback about the past behaviour of the participants by using a reputation system. The reputation of nodes is built up by the interaction among nodes, so by applying a trust system in WSN the interactions between network nodes are guided by the reputation of nodes. By collaboration of other sensor nodes first and second-hand information should be collected for computing trust value. Through observing and watch guarding technique, observing the nodes perimeter neighbouring node the direct trust or first-hand information is achieved. Whereas, the second-hand information or the indirect trust is reported by other sensor nodes in which the trust value of each node is computed by some formula combining first and second-hand information. The node will be allowed to participate in the application if the computed trust value of node be greater than some threshold, otherwise, it will be isolated from network by dissipating nodes reputation to other sensors.

To implement this system there are various challenges: to collect the first-hand information sensors should awake longer than before, this issue decreases the sleep time of watch dog nodes and their lifetime. Using second hand information is more costly because it should be transmitted proactively or reactively. The energy consumption of second-hand information depends on density and distance of sensor nodes from CHs and the BS, the transmission quality of the information, type and range of trust value, and protection mechanism to assure integrity, freshness and authentication. Next challenging issue is that reputation-based systems should deal with the accuracy of second-hand information, a malicious node that participates in the reputation system can degrade the systems fidelity by lying. Although, second-hand information is not totally dependable, it cannot be ignored because reputation systems that depend on only first-hand information have very large convergence time. Therefore, reputation systems must be able to prevent false accusations or false praise reports.

Josang and et al in [34] proposed the Beta Reputation System, where some trust-based security schemes relay on Bayesian formulation as beta reputation system for trust evolution. Prior probabilities of binary events can be represented as beta distributions which are composed of the two parameters α and β. The beta distribution f (p|α, β) can be expressed by the gamma function Γ as:

f (p|α, β) = ((Γ(α+β))/(Γ(α)+Γ(β)))$p^{\alpha-1}$(1-)

where, $0 \leq p \leq 1$, α > 0, β > 0

Trust-based LEACH schemes combine the trust management methods with various phases of LEACH in conjunction with cryptographic-based mechanism, which present more reliable variations of LEACH. This scheme only elects the nodes energy is larger than some threshold to solve the energy problem and avoids the CH re-election overhead and data losses as a result of CHs death.

VII. SECURE EXTENSIONS OF LEACH

A. S-LEACH

It is a secure extension of LEACH which consists of four phases: the advertisement phase, cluster set-up phase, schedule creation phase and data transmission phase [29]. In advertisement phase, authentication of the candidate nodes is done by the BS to avoid an attacker to advertise itself as a CH. An encrypted message is sent to the BS by each CH candidate and to one-hop neighbour by broadcasting. Using the key of the claimed node the BS checks if it can decrypt. The CH candidate will be a member of WSNs if the BS can decrypt the packet and finds the correct value otherwise it discards the packet as the CH candidate may be an attacker. Later the BS verifies that the CH

candidate has been a CH in last several rounds or not. If it has, then the BS discards the packet otherwise, it registers the CH and sends a message to these CH candidates by modified immediate authentication TESLA protocol. In cluster set-up phase the sensor nodes decides which clusters it belongs to and registers its information to the BS. Then the BS generates and sends a subkey which, generated by the secret of a sensor node, to relative CH candidate. Then a sensor node can authenticate the CH candidate by the subkey. In Schedule Creation Phase the CH sends CDMA code and TDMA schedule in encrypted form to each sensor node. In data transmission phase, the clusters are created and the TDMA schedule is fixed. Since each CH shares a subkey with each member, the data transmission in the cluster is secured.

B. Sec-LEACH

Sec-LEACH is a protocol for securing LEACH-based networks which achieves baseline security by adapting random key pre-distribution and μTESLA. A large pool of keys is generated in this scheme prior to network deployment. A ring of few keys is drawn pseudo randomly from the pool, without any replacement and assigned to each node. Each node is assigned a pairwise key shared with the base station and a group key that is shared by all members of the network prior to the deployment. After that following modifications are applied in the LEACH clustering algorithm. Initially, each self-elected CH broadcasts advertise message including keys information in its key ring where, the broadcast is authenticated leveraging on the BS who is trusted and has more resources. The remaining nodes now cluster around the closest CH with whom they share a key. A self-elected CH broadcasts its id, a nonce, and a MAC produced using the key the CH shares with the BS. The BS waits to hear and authenticate the modified advertise messages from all CHs, then compiles the list of legitimate CHs and sends the list to the network using μTESLA [30].

Ordinary nodes now know which advertise messages they received are from legitimate nodes, and can proceed with the rest of the original protocol by choosing the CH from the list broadcast by the BS. Afterwards, ordinary nodes compute the set of CHs key ids, choose the closest CH with whom they share a key and send it a join request message protected by a MAC. In the setup phase, the CHs broadcast the time slot schedule to the nodes choose to join their clusters and this broadcast is authenticated as before. In the steady-state phase, node-to-CH communications are protected using the same key used to protect the join request message. The CHs can now check the authenticity of sensing reports they receive, perform data aggregation, and send the aggregate result to the BS. The aggregate result is protected using the symmetric key shared between the CH and the BS. To have freshness, a counter shared between the CH and the BS is included in the MAC value.

C. SC-LEACH

This secure LEACH protocol tries to produce optimal CHs in each round and to improve the security of routing uses a pre-shared key pair. A candidate CH broadcast with plain text, the sequence of present round and the number of all nodes which has ever been CHs, as well as the ID of every key in the key ring. Then the node selects the CH based on the received signal strength. Node afterwards records the key flag of the selected cluster, determines the key S relative to itself and sends sequence S to the CH to declare its participation and inform the CH the key S. Based on the number of nodes registering in a cluster the CH allocates TDMA time slot. The cluster members start data acquisition in their own TDMA time slot and encode the data and send them to other CHs. Once a frame is completed, the CH decodes the data, run data fusion algorithm, and sends it to BS. By dispatching pre-shared key pair to the nodes, the key pair between any two nodes is only shared by themselves. Other nodes do not know the key, so the

capture of one node would not lead to the leakage of any secure path built indirectly [28].

D. GS-LEACH

GS-LEACH or grid-based secure LEACH uses pre-deployment key distribution using prior knowledge of the deployment area. It uses grid-based deployment where a certain number of sensors are deployed randomly around each point of a grid. The sensors around a grid point form a cluster for local data compression and take turns as CHs to communicate with the BS. For secure data transmission, each of the n sensors is given a set of m randomly selected keys from a large key pool, which it uses for communication with the group members. Depending on the key pools of two sensors in a group, the probability that two given sensors communicate, affects security as well as the performance of the network. An additional key is also given to each sensor for communication with the BS. In the setup phase, each sensor decides to elect itself as CH with the probability function, such that there is only one CH per grid point. Then CH broadcasts an advertisement message using its id, id_H and a nonce to avoid replay. Each non-CH in the group uses the PRNG with id_H to generate the m keys of the CHs to receive advertisements, and checks for a common key. Each node chooses the CH that it has at least one common key with. It sends out a join request message which is protected by a MAC that is generated using the common key between this node and the CH. CHs send out a time schedule to the members, sensors transmit during the given slot and are in monitoring mode other times to save energy. During the steady-stage phase members send encrypted data to the CH.

E. Armor-LEACH

It is an energy efficient secure scheme designed by Abuhelaleh et al. [35], in which they combine Sec LEACH and Time Controlled Clustering Algorithm (TCCA). The Armor LEACH is divided into five steps of Setup phase and Steady State phase. A group of keys is assigned to each sensor prior to deployment and each sensor assigned by a pairwise key share with the BS. The Key Group Size (KGS) which is to be assigned to each sensor is fixed and the Key Pool Size (KPS) has direct impact on the sharing key probability between sensors and security level. When KGS is fixed, the size of KPS will affect this probability; the larger the KPS, the smaller the KPR [36]. Also, the probability that a link is not compromised is given by following formula:

$$\text{Security Level} = 1 - \frac{KGS}{KPS}$$

Thus, larger KPS provides higher security level. To determine the eligibility of each sensor to become a CH at the beginning of each round, each sensor generates a random number between 0 and 1 and it is compared by threshold value T(S). If the value of T(S) is greater than random number, sensor becomes CH. In Setup phase, each elected CH broadcasts an advertising message to its neighbours announcing that it is a CH. When a sensor receives the message, it chooses a key shared with CH to use in the current round, and it forward the message simultaneously to its next neighbours. Then sensors send join request to the CH. The request message consists of sharing key ID; join request message, the remaining TTL value, and the encryption of sensor ID, CH-ID, sharing key ID and the nonce sent by CH. The encryption is produced using message authentication code uses the sharing key. TTL with time stamp helps CH to form a multi-hop view of its clusters, to create a collision-free transmission schedule. After that CH broadcasts its ID and the time slot schedule for each sensor in its cluster. The communication begins in steady state phase and each sensor sends its report to its CH that consists of sensor ID, CH ID, sensor report, and the encryption of sensor ID, CH ID, sensor report, and the nonce with its reporting cycle within the current round. The encryption is produced using the same MAC which is produced in setup phase. Then CH sends the aggregation of sensors reports to the BS which consists of CH ID, BS ID, the aggregation of sensors reports, and the encryption of the aggregation

report, encrypted using MAC produced by the sharing key between CH and the BS. Using random key distribution (RDK) to create sharing keys leads to match most of sensors with available CHs. The message in the second step of the setup phase, is encrypted with a key from the key pool, CH can conclude that they came from legitimate sensor by successfully decrypting the message. Also, by the counter value shared between the CH and the BS in steady state phase, the freshness is guaranteed. The biggest security issue in Armor-LEACH is the resiliency against sensor captures, where the link keys used for sensor-to-CH communications are not pair-wise in Armor-LEACH.

F. R-LEACH

It is a cryptographic version of LEACH proposed by Zhang et al. in [37], where this scheme bootstraps its security from improved random pair-wise keys (RPK) scheme which relays on symmetric keys for node-to-node authentication. RLEACH is composed of five phases. In Pre-distribution phase, each node is pre-distributed with its ID and an original key where, each node can use those keys as the shared-key with the other nodes, and register the corresponding ID of the shared-key. The record of every nodes ID, whole net key pool and one-way hash function F should be stored by the BS. The node distributes m keys to its neighbour nodes by choosing m neighbour nodes from its neighbour group. If the nodes are in the same group, there is no need to pre-distribute pair-key for them because they have the same public seed and hash function in common. Nodes in the same group can use the m to calculate the shared-key for their communication. If nodes are in different groups, they can use Hash function to compute the shared-keys and store the related node identifiers at the same time. In Shared- key discovery phase node broadcasts its ID to its neighbour nodes. The Cluster set-up phase of RLEACH is the same as LEACH. In Schedule creation phase, CHs with all member nodes setup secure links. In Data transmission phase to ensure the security of data transmission, the CH and the member nodes use the shared-key for authentication each other. The CH integrates and compresses received data to a new signal, and then send it to BS with its ID. BS will use the key Ki to validate whether the data is effective.

G. s-LEACH

It is a secure LEACH scheme which relay on Jake Channel Scheme (JCS) as proposed by Jangra and et al in [38], which uses Received Signal Strength or RSSI for Sybil attack detection, that can be recognized by change in the number of CHs. In this scheme firstly, by finding the number of CHs as compared to threshold value intruder is detected. When CH receives broadcast information from other CHs during the CH election, it will register them. It may a sign of Sybil attack if the number of CHs is bigger than a definite threshold. When CH sends TDMA allocation to its members, it informs that Sybil attack happened and after that Sybil node discovering method will be started in the network. The signal strength RSSI is the function of sending-receiving distance d, in Jake channel space. It is possible to decide whether or not there is Sybil attack, after calculating the position of nodes with the signal strength. The power prices $RSSI_t$ of nodes are often thought to be identical at identical time and remains unchanged.

H. LS-LEACH

LS-LEACH is a secure and energy efficient routing protocol called as Light-weight Secure LEACH [39]. In this scheme authentication algorithm is integrated to assure data integrity, authenticity and availability. Initially, each node is equipped with two keys: one is shared with the BS and the second is shared with all nodes for the initial phase to be used for cluster joining process. The CHs are elected and use their private key to communicate with the BS. Nodes use their group key to request joining the intended clusters. After forming the clusters, the CH can update the cluster key providing a different key than the initial ones. Also, the BS can update the CHs private key if required. Electing a node for next round

CH should be done before the end of the current round. The current CH verifies the authenticity of the new CH to the BS and to the nodes where, the message from the CH to BS is encrypted by MAC algorithm with the shared key between the BS and CH. After that the BS broadcasts the list of the authenticated CHs to all nodes using μTESLA. The selection of CH should be based on the distance between the clusters and the node to reduce the energy required when communicating with each other.

At the beginning of a new round, the CH sends a verification message (verification[M]) with key (K_{N-N}) to neighbour nodes. After receiving the message, nodes reply to the CHs request by a verification message encrypted by the shared key ([K_{N-N} , authentication [M]]) requesting to join the cluster. However, the CHs needs to make sure that it doesn't allow the number of nodes to exceed the allowed number in cluster ($N_i \leq 20N_i$). On the other hand, nodes must require to join the clusters closer to them to reduce the energy consumption in receiving and transmitting. Sensing takes place when the nodes are sensing the environment. Listening/Transmitting happens when nodes are expecting to have communication with the CH or BS. Sleeping takes place when the nodes are not in sensing, listening/transmitting modes. This requires the nodes to be in sleep mode to avoid the overhearing which consumes node energy. Nodes are required to have a log for the connections attempts that are initialized with them. When the attempts reach the predefined threshold, a flag is raised to the CH and the BS. The BS has to perform the necessary actions in case the sensor is under attack.

I. LEACH-TM

Weichao and et al in [40] has presented LEACH-TM, in which active trust transmission is used to design an improvement of LEACH which solves the problem of real times, decentralizes network load, and trust loss in traditional mechanism. To enhance the robustness of the network this scheme adds a CH adjusting procedure which equilibrates the distribution of CHs. Trust in this scheme is the integration of direct and indirect trust which ranges from 0 to 1. For trust computation a weight factor is assigned to each direct and indirect trust and T_{A-B} which is the Trust of A to B. In this scheme only nodes whose energy is larger than the energy threshold is eligible to be CH. When a node decides to be CH, it broadcast a notice, including its ID and remaining energy. After receiving this notice, non-CH nodes insert the node ID into their set of standby CHs, while CH constructs its neighbour CH table. Then, CH determines the distance of neighbouring CH by received signal strength. If the distance is smaller than L, then *Nclose* = true; else *Nclose* = false. For clustering, a CH counts the number of close neighbours as N. If N > 0 then it computes the weight of each neighbour. After choosing the node whose weight is the heaviest, a cancelling packet which is used to cancel the node itself as CH is constructed and transmitted at a time randomly chosen from 0 to *T1*. When all CHs have been designated, non-CH node decides its own CH from its CH set. Then the procedure is the same as LEACH.

J. TLEACH

Authors in [41], proposes a trust-based solution TLEACH where, to reduce energy consumption it uses CH-assisted monitoring. This scheme is a modified trust-based version of LEACH in which it combines a trust management module with trust-based routing module and it consists of monitoring module and trust evaluation module. In set-up phase, the advertisement section is same as the original protocol but the CH selection is based on the decision trust in cluster joining phase. Firstly, the decision trust about CH selection operation is computed by each CH candidate and find out the trust list of CH candidates. After that CH is chosen from the trust list which trust is maximal, because all the CH candidates may be malicious, a trust threshold is defined and the

candidate of maximal trust beyond the threshold is selected. If there are no candidates whose trust values are beyond the threshold, the nodes reset the CH selection. Finally, the non-CH nodes send cluster-join messages to their CHs. In Confirmation phase, CHs create a TDMA schedule and adjust the schedule to support trust evaluation, adding trust slots.

The steady-state is divided into frames, consisting data slots to send data and trust slot to evaluate and exchange trust. The non-CH nodes send data to their CHs in their data slots and control monitoring module to observe neighbours' behaviours, while the CHs keep their receivers on to receive the data, and all nodes perform trust evaluation during the trust slots. In Data slots, CHs keep their receivers on to receive data. In the last data slot, CHs aggregate data based on the trust. Non-CH nodes send data to their CHs during their time slots, and the monitoring modules are turned off and when not in their time slots, they turn it on with a monitoring probability. The CHs keep observing their members behaviours, while holding the most comprehensive information about clusters, and the non-CH nodes get SHT from their CHs. If the CHs have high trust, the cluster-members can turn off their monitoring modules in most time, as they can get trustworthy information about neighbours from CHs. Otherwise, the members need to get trust by direct observations with high monitoring probability. CHs perform trust evaluation and update their NSTTs (Neighbours Situational Trust Table) and they share their observations by broadcasting their situational trust values to their members. Non-CH nodes evaluate direct trust by the misbehaviour reports of their monitoring modules and indirect trust by SHT received from their CHs.

K. CS-LEACH

Yang et al. presented a trust-based extension of LEACH Centralized Secure LEACH [42]. They implemented the use of a Key Distribution Centre (KDC), where each node shares a unique private key with the gateway for broadcast authentication. This scheme consists of rounds here, each sensor possesses two permanent keys, a gateway private and a node private key (KP). The node waits for a message at the beginning of a round, as they enter the network. A Round Start Message functions as a synchronization message is triggered from the gateway in each round in which the message distributes a session template and a network key used to produce session key and MAC keys. The communication between nodes and the gateway, and a CH and a cluster member is encrypted by the Session Key. To encode a MAC to provide integrity protection the MAC Key (KMAC) is used. The KMAC for each round is unique and a new KMAC depends on KN which is part of the Round Start Message hence, the Round Start Message is unique. To reject malicious nodes and prevent them to be a CH which is encrypted with the gateway session key to prevent replay attack, gateway distributes a blacklist to warn nodes in Cluster Setup Phase.

Some nodes self-elect to become CH once nodes receive this blacklist, other nodes select a CH based on CH signal strength, and reject nodes listed by the blacklist. To ensure data confidentiality the CH must acquire session key for its members, before a member starts transmitting data to a CH. In this stage, gateway can associate members with CHs and scan to duplicate IDs and select members for Trust Checks (TC) from each cluster. The gateway does not issue the session key, if a cluster member has insufficient trust. Once the keys are compiled, a response message is sent that is encrypted using the CHs private key. CH is responsible to assign time slots to members to transmit their data to CH. In addition, members should maintain a MAC of all transmission for a given round called TC. The CH aggregate data and send it to gateway. This aggregation must be lossless to ensure the gateway is able to retrace the source node ID of sensor data. This is important for the gateway to produce a MAC to be compared to the TC produced by a member. After a round, the gateway evaluates

the performance of nodes and is able to reproduce a TC for each cluster member based on the data sent by CHs. When TC validation fails, both the CH and the cluster member must be punished. For trust management issues, CSLEACH uses two thresholds termed CH Trust Threshold (CTT), and the Member Trust Threshold (MTT).

VIII. CONCLUSION

Security in WSNs has become a new area of research and introduce unique challenges in designing of protocols as compared to traditional wireless networks such as mobile, ad hoc and cellular network. In this paper, we identified some of the goals of security as well as various attacks in WSNs from recent works. We analysed a cluster-based routing algorithm LEACH, discussed some of its extensions as well as secure extensions and classified secure extensions as cryptographic based and trust-based schemes. In cryptographic based LEACH, mostly nodes use keys for data transmission from sensor nodes to base station or base station to the nodes. By using such keys sensor networks are only protected from outsider attackers but for insider attackers trust-based schemes are used which combines reputation management systems with LEACH. However, when compared with traditional LEACH protocol all of these secure LEACH has some limitations such as they use extra energy for key management, reputation management systems since sensor nodes have limited energy. Future perspective of this work is to modify above routing protocol in order to make them more energy efficient and secure.

IX. REFERENCES

[1] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less Low Cost Out Door Localization for Very Small Devices," Tech. rep. 00729, Comp. Sci. Dept., USC, Apr. 2000.

[2] A. Savvides, C.-C. Han, and M. Srivastava, "Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors," Proc. 7th ACM MobiCom, July 2001, pp. 166–79.

[3] Ian F. Akyildiz and Mehmet Can Vuran, Wireless Sensor Networks c 2010 John Wiley & Sons, Ltd.

[4] Siva D. Muruganathan, Daniel C. F. Ma, Rolly I. Bhasin, and Abraham O. Fapojuwo "A Centralized Energy-Efficient Routing Protocol for Wireless Sensor Networks", IEEE Radio Communications March 2005.

[5] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," Proc. 33rd Hawaii Int'l. Conf. Sys. Sci., Jan. 2000.

[6] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), year 2006.

[7] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks," Proc. 5th ACM/IEEE Mobicom, Seattle, WA, Aug. 1999. pp. 174–85.

[8] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks," Wireless Networks, vol. 8, 2002, pp. 169–85.

[9] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[10] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," Proc. ACM Mobi-Com 2000, Boston, MA, 2000, pp. 56–67.

[11] D. Braginsky and D. Estrin, "Rumor Routing Algorithm for Sensor Networks," Proc. 1st

Wksp. Sensor Networks and Apps., Atlanta, GA, Oct. 2002.

[12] S. Lindsey and C. Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information Systems," IEEE Aerospace Conf. Proc., 2002, vol. 3, 9–16, pp. 1125–30.

[13] A. Manjeshwar and D. P. Agarwal, "TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks," 1st Int'l. Wksp. on Parallel and Distrib. Comp. Issues in Wireless Networks and Mobile Comp., April 2001.

[14] A. Manjeshwar and D. P. Agarwal, "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks," Proc. Int'l. Parallel and Distrib. Proc. Symp., pp. 195–202.

[15] J. N. Al-Karaki et al., "Data Aggregation in Wireless Sensor Networks — Exact and Approximate Algorithms," Proc. IEEE Wksp. High Perf. Switching and Routing 2004, Phoenix, AZ, Apr. 18–21, 2004.

[16] S. Capkun, M. Hamdi, and J. Hubaux, "GPS-free Positioning in Mobile Ad-hoc Networks," Proc. 34th Annual Hawaii Int'l. Conf. Sys. Sci., 2001 pp. 3481–90.

[17] Y. Xu, J. Heidemann, and D. Estrin, "Geography informed Energy Conservation for Ad-hoc Routing," Proc. 7th Annual ACM/IEEE Int'l. Conf. Mobile Comp. and Net., 2001, pp. 70–84.

[18] B. Chen et al., "SPAN: An Energy-efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks," Wireless Networks, vol. 8, no. 5, Sept. 2002, pp. 481–94.

[19] Y. Yu, D. Estrin, and R. Govindan, "Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks," UCLA Comp. Sci. Dept. tech. rep., UCLA-CSD TR-010023, May 2001.

[20] I. Stojmenovic and X. Lin, "GEDIR: Loop-Free Location Based Routing in Wireless Networks," Int'l. Conf. Parallel and Distrib. Comp. and Sys., Boston, MA, Nov. 3–6, 1999.

[21] Tahir Naeem, Kok-Keong Loo, Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks, International Journal of Digital Content Technology and its Applications, Page 89-90 Volume 3, Number 1, year 2009.

[22] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[23] Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page53-57, year 2004.

[24] Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication Technology (ICACT), Page(s):6, year 2006

[25] Md. Solaiman Ali, Tanay Dey, and Rahul Biswas, "Advanced LEACH Routing Protocol for Wireless Microsensor Networks", Department of Computer Science & Engineering Khulna-9203, 5th International Conference on Electrical and Computer Engineering ICECE 20-22 December 2008.

[26] Muhammad Omer Farooq, Abdul Basit Dogar, Ghalib Asadullah Shah," Multi-hop Routing with Low Energy Adaptive Clustering Hierarchy", 2010 Fourth International Conference on Sensor Technologies and Applications, IEEE Computer Society.

[27] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Micro-Sensor Networks", Proceedings of the 33rd Hawaii International Conference on System Sciences – 2000.

[28] Wang, J, Yang, G, Chen, S, Sun, Y., Secure leach routing protocol based on low- power

cluster-head selection algorithm for wireless sensor networks, Inter- national Symposium on Intelligent Signal Processing and Communication Systems, 2007, PP.341-344.

[29] Xiao-Yun W, Li-Zhen Y, Ke-fei C., "SLEACH: Secure Low Energy Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks", Wuhan University Journal of Natural Sciences 2005;10(1):127–31.

[30] Oliveira LB, Ferreira A, Vilaca MA, Wong H C, Bern M, Dahab R, Loureiro, "Sec LEACH On the security of clustered sensor networks", Journal of Signal Processing 2007:2882–95.

[31] Xiao Y, Rayi VK, Sun B, Du X, Hu F, Galloway M., "A survey of key management schemes in WSNs", journal of Computer Communications 2007.

[32] Simplcio Jr MA, Barreto PSLM, Margi CB, Carvalho TCMB, "A survey on key management mechanisms for distributed Wireless Sensor Networks", Journal of Computer Networks 2010.

[33] Zhu, S, Setia, S, Jajodia, S, "Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", 10th ACM conference on Computer and communications security, 2004.

[34] Jøsang, A and Ismail, R., "The Beta Reputation System", 15th Bled Electronic Commerce Conference Bled, Slovenia, 2002.

[35] Abuhelaleh, MA, Mismar, TM, Abuzneid, AA, "Armor-LEACH – Energy Efficient, Secure Wireless Networks Communication", 17th International Conference on Computer Communications and Networks, 2008.

[36] Abbasi AA, Younis M, "A survey on clustering algorithms for WSNs", Computer Communications 2007.

[37] Zhang, K, Wang, C, Wang, C., "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management".

[38] Jangra, A. Swati, Priyanka, "Securing LEACH Protocol from Sybil Attack using Jakes Channel Scheme (JCS)", International Conference on Advances in ICT, 2011.

[39] Muneer Alshowkan, Khaled Elleithy, Hussain AlHassan, "A New Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks", Department of Computer Science and Engineering University of Bridgeport, USA.

[40] Weichao, W, Fei, D, Qijian, X, "an Improvement of LEACH Routing Protocol Based on Trust for Wireless Sensor Networks, 2009, 5th Conference on Wireless Communications and Mobile Computing, 2009, PP.1-4.

[41] Bhuvaneswari PTV, Vaidehi V, "Enhancement techniques incorporated in LEACH- a survey", Indian Journal of Science and Technology 2009.

[42] Yang, Li, "Centralized security protocol for wireless sensor networks", Master's Project, San Jose State University, spring 2011.

Cite this article as :

Saziya Tabbassum, Sanjeev Bangarh , "A Survey on Attacks, Security Mechanisms and Secure Extensions of Hierarchical Clustering Based Sensor Networks", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 1, pp. 05-24, January-February 2022. Available at doi : https://doi.org/10.32628/CSEIT2176108
Journal URL : https://ijsrcseit.com/CSEIT2176108