Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.3 Year 2018
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

Comp Page 38 - 55

Methods of Secure Routing Protocol in Wireless Sensor Networks

Waleed Kh. Alzubaidi
Dep. Informatics Institute
University of Information Technology and Communications, Iraq
(waleed8010@gmail.com)

Shaimaa H. Shaker
Dep. of Computer sciences
University of Technology
Baghdad, Iraq
(120011@uotechnology.edu.iq)

Recived : 17\7\2018 **Revised : 1\8\2018** **Accepted : 16\8\2018**

Available online : 26 /9/2018

DOI: 10.29304/jqcm.2018.10.3.437

Abstract:

The Wireless Sensor networks (WSN) consider an emerging technology that have been greatly employed in critical situations like battlefields and commercial applications such as traffic surveillance, building habitat, smart homes and monitoring and many more scenarios. Security is one of the main challenges that face wireless sensor networks nowadays. While an unattended environment makes the deployment of sensor nodes in the networks more vulnerable to vary of potential attacks, the limitations of inherent power and memory for the sensor nodes makes conventional solutions of the security is unfeasible. The sensing technology combined with processing power and wireless communication makes it profitable for being exploited in great quantity in future. The wireless communication technology also acquires various types of security threats. This paper discusses a wide variety of attacks in WSN and their classification mechanisms and different securities available to handle them including the challenges faced.

Keywords-Wireless Sensor Network; Security Goal; Security Attacks; Defensive mechanisms;Challenges

1. Introduction

This paper presents a thorough picture of Wireless Sensor Network (WSN), grid-based cluster, and role of sensors in WSN. Additionally, the security issue concern in WSN embraced with several kinds of attacks in WSN is described. Then tailed by several authenticated routing protocols and the routing framework. Finally,in the last portion of this paper, the literature survey on intelligent routing for clustered WSN is discussed. An overview of the current paper is depicted in Figure 1.

2.1 Wireless Sensor Network

A WIRELESS sensor Network (WSN) is a self-sufficient, self-arranging, and multi-hop network that encompasses a significant quantity of sensor nodes. The sensor nodes work together with each other to screen the physical condition around them. WSNs are ordinarily unattended and energy compelled in nature. Accordingly, they require energy efficiency and efficientprotocols to expand the system lifetime and tasks [1]. A WSN contains a few sensor nodes, which can be exploited as a mass of various application situations, for example, agriculture, military, health care, and energy. WSN has been used as a piece of various fields such as schools, colleges, battlefields, surveillance and so forth. It has been used as a piece of everyone's day to day life and its provisions are growing in well-organized fashion. WSN has come in presence as a key solution for a few issues where human mediation is difficult.

The fast advances in wireless technology, implanted chip, incorporated micro-electro-mechanical systems (MEMS), and nanotechnology has engaged the progression of nominal effort, low-control, and, multifunctional sensors. Sensors are of little in size and can perform event identification, data tracking, interacting with each other or with the data sinks. Sensor nodes are associated with each other through the wireless medium, for example, infrared or radio waves and it becomes operational with application data arrival/sensing. Internal memory related to every sensor node stores the data of its related event packets. A group of sensors sharing a wireless medium form a WSN for gathering information and transmitting it to remote clients (sinks). The principle motivation behind the WSN is to screen and gather information from the sensors and after that transmit this information to the sinks [2]. WSNs are more appealing because of their wide range of utilization, like weather monitoring, military surveillance, health care, disaster management etc. The essential reason for WSN growing popularity was to ceaselessly screen such conditions that happen to be extremely difficult or unrealistic by people [3].

The exploration of WSNs is a subset research area of Internet of Things (IoT). The sensors ought to be allocated with a routing protocol such that the information is transmitted to the end-client by means of various intermediate sensors nodes.

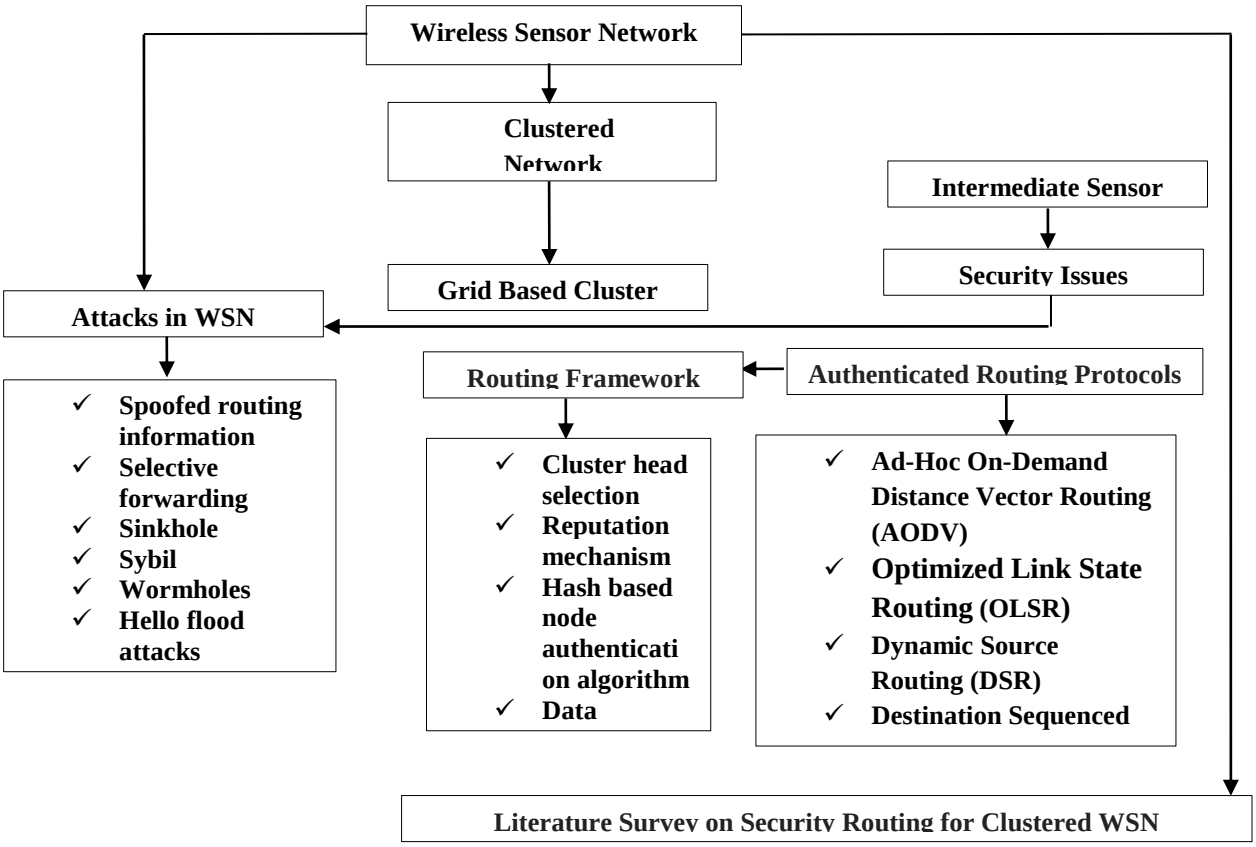

Figure 1: Literature Review Framework

A WSN may comprise of a few heterogeneous sensor nodes to perform dedicated assignments conveyed in a territory of intrigue. There exist numerous proprietary and nonproprietary existing solutions for fetching sensed information from the sensor nodes. In any case, the present pattern of utilizing IP-based sensor organizing arrangements, (for example, 6LoWPAN and IPv6) empowers the WSN to be associated with the web. Therefore, WSNs can be utilized for observing/controlling diverse applications through the web based network, which in turn, builds up the idea of the Internet of Things (IoT) [4]. In sensor nodes, the fault may occur because of the incorrect condition of equipment or a program as an outcome of a sudden fault of any part. Also, any performance degradation for nodes happening due to energy exhaustion is critical and as the time advances these shortcomings may increment, bringing about a non-uniform system topology. The issues that can happen because of the failure of sensor nodes are misfortune in availability, delay because of the misfortune in association and partitioning of the system because of the gap created by the failed sensors [5].

2.2 Clustered Network

Clustering was proposed in early researches [6] as a mean of enhancing WSN lifespan and was immediately embraced in progressive works. In clustered networks, a few nodes move towards becoming Cluster Heads (CHs) and are in charge of directing messages from other cluster CHs and cluster member nodes. Nodes that are not CHs moved toward becoming cluster member nodeand send messages just to CHs. Clustering was introduced to reduce the general power utilization and expand network lifetime. Thought of clustering seems to be self-explanatory and so apparent that it was fixed deeply into WSN theory. Clustering strategies are additionally one of the means to covenant with topology control, which can compose a WSN into a group based system. Task scheduling, data gathering, and Transmission Power Control algorithms can be executed in this structure with a specific end goal to accomplish particular task. A clustering algorithm can partition sensors into various clusters/gatherings/subgroups.

In each cluster, a CH is chosen to be responsible for producing a transmission plan, gathering information from every one of the sensors in the group and transmitting the amassed data back to the Base Station (BS). In light of the grouped structure, the framework can provide extended network life by keeping minimum communication among the sensors within a cluster, without affecting the usefulness of the system. The CH is the developer of a cluster and it is accountable for social affair information and transmitting the information to the BS. The CHs will possess more energy than ordinary cluster member sensors and in this manner, can better control the network for longer period. In many scenarios, CHs also take part to adjust the power utilization on participating sensors. Which sensors should be chosen as CHs requires cautious examination. In general, one of three CH race plans is adopted as : a) Deterministic, b) Random, and c) Adaptive. Subsequent to being chosen, the CHs will publicize themselves by communicating their data to different member sensors. Every sensor will assemble the data from all the CHs inside its radio coverage range and after that choose which CH to join in view of some correspondence properties. A few measurements can be utilized to decide the correspondence properties between a sensor and a CH, for example,

2.3 Grid Based Cluster

Many grid-based algorithms have been developed. The author [7] displayed a calculation called Low Power Grid-based Cluster Routing Algorithm (LPGCRA).It chooses the CH among the typical sensor nodes which have maximum residual energy. Regardless of the fact that LPGCRA focuses to balance the overall load of the network, it has the accompanying limitations. On the off chance that the CH is far from every single other sensors in a group, then all member sensors need to spend more energy including CH itself. Also, CHs transmit accumulated local information specific to the sink node which is moderately less in number than the cumulative amount of sensor nodes, prompting fast battery exhaustion of the CHs. In another framework based approach called Grid Based Routing (GBR), has endeavored to expand the system lifetime by ideal determination and dispersion of the CHs over the objective zone. Nevertheless, they expect a settled number of grids which may not be sensible for a huge region of operation. Besides, in the selection phase, CHs are chosen based on the sensor node’s transmission time to the sink. In this way, the technique chooses the CHs which are close to the sink in every grid and thus the member sensor nodes of the cluster exhaust their energy faster for entire transmission to the CH. However, none of the above algorithms address the energy efficiency, load matching and fault lenient secure routing issues together [8]. Grid network with clustering techniques showed better outcomes in contrast with the grid network without clustering. It requires less energy usage than other [9] available methods.

Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.3 Year 2018
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

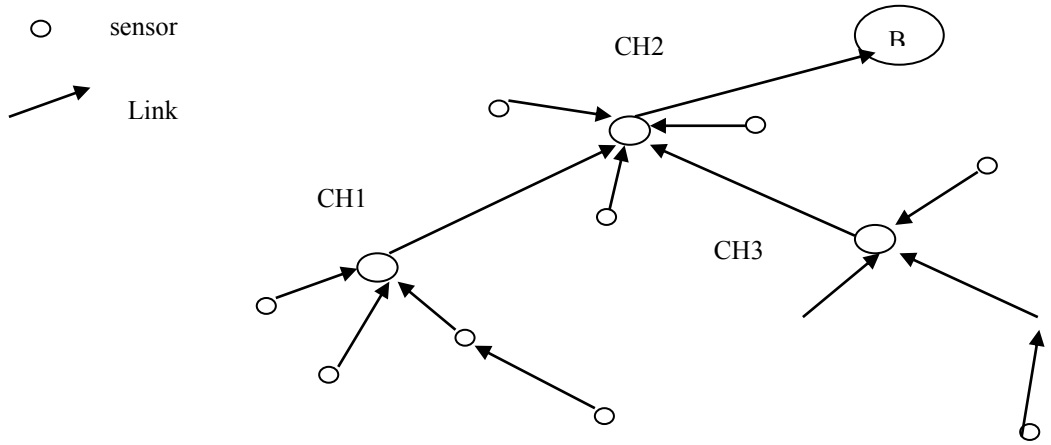

Figure2. Representation of Cluster Based WSN

2.4 Intermediate sensors in WSN

The mix of heterogeneous sensors creates a key innovation for the 21st century named WSN which gives phenomenal open doors in many areas running from military to agriculture and has applications in events like , health monitoring, modern control and home systems.As compared to other type of wireless communication technologies, WSN requires utilization of sensor systems to transport the stream

Security is a vital issue to be considered for the system which is conveyed in threatening condition. Organization of a system in a human uninterruptible place is extremely vulnerable without security. Plan of a security convention is a testing errand because of the nature and accessibility of assets. Security instruments utilized for systems can differ as per the diverse needs ranging from fixed to wireless networks [12].

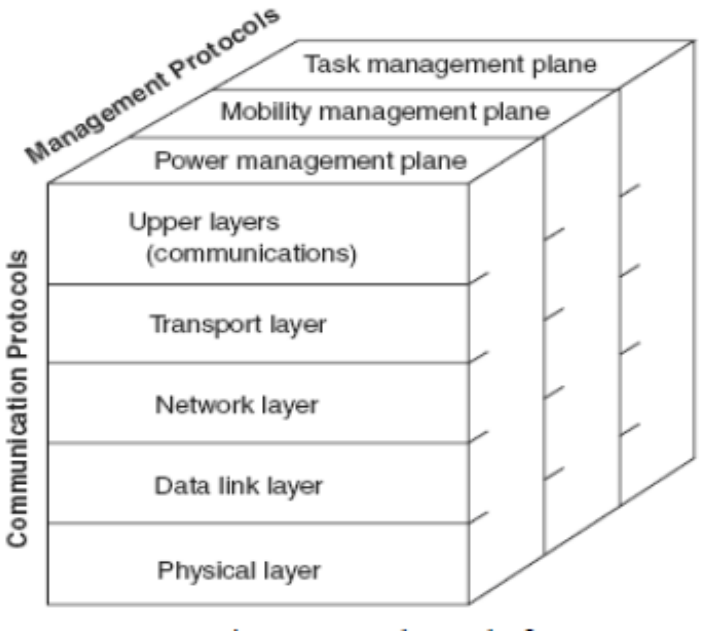

Figure 3. Representation of Generic Protocol Stack for wireless sensor Networks

of detected information from numerous districts (sources) to a specific sink [10].Sensors are the genuine interface to the physical world, in other words, the modern gadgets that can watch or control physical parameters of the earth.In this context, without the intermediate sensor nodes, which helps to carry forward data en route, a remote sensor system would be irrelevant totally. Any sensor or actuator, which is part of WSN can act as an Intermediate sensor based on their location and data transmission path.Thus, Intermediate sensor nodes are in charge of self-sorting out a suitable system foundation, with multi-hop data forwarding between actual source and destination sensor nodes. In this way, WSNs can operate with little, minimal effort gadgets for an extensive variety of uses and they don't depend on any previous infrastructure [11].

2.5 Security Issues

Security is a vital issue to be considered for the system which is conveyed in threatening condition. Organization of a system in a human uninterruptible place is extremely vulnerable without security. Plan of a security convention is a testing errand because of the nature and accessibility of assets. Security instruments utilized for systems can differ as per the diverse needs ranging from fixed to wireless networks [12].

An arrangement of standards for tending to the issue of securing remote sensor systems was proposed. A solution with regards to these standards, underpins a differential security benefit that can be powerfully arranged to adapt to changing system state. Security of a system is controlled by the security over all layers. In a massively distributed network, safety efforts ought to be agreeable to dynamic reconfiguration and decentralized administration. In a given system, at any given instant, the cost brought about because of the safety efforts ought not to surpass the cost surveyed because of the security dangers around them. If physical security of nodes in a system isn't ensured, the safety efforts must be strong to physical altering nodes in the field of deployment. Since sensor systems posture extraordinary difficulties, the security strategies as a part of conventional systems can't be utilized straightforwardly. On account of different limitations in WSN, the accompanying perspectives ought to be painstakingly considered when planning a security plot: Power efficiency, Node Density and Consistency, Adaptive security, Self configurability, Simplicity and local ID [13]. Security in WSNs is as essential as in different styles of frameworks, particularly in military and security applications (e.g. intruder recognition). Aggressors may endeavor to block movement in destinations (i.e. execute a denial of service attack) or deal information with the expansion of some satirize detected information to arrange (i.e. aggregating invasion). Aggressors from the inside (ruined node already situated into WSN) can confer steering issue by driving information development to parodied sinkholes. In WSNs, different assaults are discovered in the following section that damages the normal operation of the entire system framework.

3 Attacks in WSN

3.1 Spoofed routing information

The most direct attack against a routing protocol in any system is to focus on the routing information itself while it is being traded between nodes. An aggressor may spoof, modify, or replay routing data, keeping in mind the end goal to upset activity in the system. These interruptions incorporate the creation of routing loops, attracting or repulsing system movement from selected nodes, broadening and shortening source routes, producing counterfeit mistake messages, dividing the network, and expanding end-to-end idleness. A countermeasure against spoofing and alteration is to affix a message authentication code (MAC) after the message. Proficient encryption and verification methods can shield satirizing attacks. In this kind of attacks, a malevolent node parodies a MAC address of a node and makes various ill-conceived identities that highly influence the normal operation of wireless sensor network [14].

3.2 Selective forwarding

WSNs are normally multi-bounce systems and consequently in view of the presumption, that the participating nodes will forward the messages dependably. Malicious or attacking nodes can however decline to course certain messages and drop them. In the event that they drop every one of the packets through them, at that point it is known as a Black Hole Attack. In any case, in the event that they specifically forward the packets, is known as selective forwarding. To counter the possible attacks associated with this, Multipath routing can be utilized. Such ways of routing are not direct as they don’t have two consecutive regular nodes, and they utilize implicit acknowledgements, which guarantee that packets

are forwarded as they were sent. In networks, attackers focus on two kinds of attacks: an information attack and a routing attack. A selective forwarding attack is a kind of information attack, in which a traded off node specifically drops a packet. In this way, a selective forwarding attack may harm the system proficiency. This kind of attack can also be thought to be a unique instance of black hole attack. Most of such attacks are caused by a malignant node that is situated in the route of information stream. Such nodes can dismiss a certain or specific delicate message that starts from different parts of the network and to be forwarded to the base station. Consequently, a malevolent node can bring down certain nodes near the base station to damage end to end connectivity. Such pernicious node specifically targets dropping delicate packets, for example, a packet that reports foe tank development. Malicious sensor nodes can work as normal sensor nodes. Selective forwarding attacks can be categorized into two classes: drop packets in certain nodes and drop packets of certain types [15].

3.3 Sinkhole attack

Contingent upon the routing algorithm method, a sinkhole attack tries to bait all the activity toward the traded off node, making a figurative sinkhole with the enemy at the middle. Geo-routing protocols are known as one of the directing convention classes that are impervious to sinkhole attacks. Such routing topology is developed utilizing just restricted data, and movement is normally directed through the physical area of the sink node, which makes it hard for an attacker to target somewhere else for making a sinkhole. In a sinkhole attack, the gatecrasher's point is to bait all the activity from a specific zone through a traded off node, to launch an attack. Thereafter, the traded off node tries to pull in all the movement from neighbor nodes in view of the direction measurements utilized as a part of the routing protocol. Sinkhole attack is one of the key routing attacks which is tough to counter on the grounds that the routing data provided by a node in a remote sensor arrangement, is hard to validate [16]. To lunch a sinkhole attack, the gatecrasher first victimize any normal node in the network and then the compromise node attacks the other neighbor nodes based on the data received from the conventional routing protocols. This leads to a serious attack situation due to the traded off nodes location proximity to the sink. As a consequence, the source is unable to send information packets to the sink . This prompts misrouting of information bundles [12].

3.4 Sybil attack

The Sybil attack signifies "damaging device illicitly dealing with several identities". The attacker adopts the procedure of making a few duplicate nodes utilizing a similar identity i.e. indistinguishable node id. For example, an inconvenient node can easily stretch false identities, or may mimic different other trustworthy nodes inside system. In particular, WSNs are more prone to sybil attack due to the nature of open and shared wireless transmission medium. In addition to that , exactly the similar rate of reappearance is being shared among all nodes. In such scenarios, the attacker could make different lacking authenticity characters by manufacturing or maybe taking these personalities with respect to trustworthy nodes. In this manner , the beds base station cannot differentiate between the legitimate and produced nodes. This befuddles the base station alongside different nodes and corrupts the system execution [17]. In this attack, a solitary node exhibits different characters to every single other node in the WSN. This may deceive different nodes, and henceforth routes accepted to be disjoint as a particular node can have a similar enemy node. A countermeasure to sybil attack is by utilizing a remarkable imparted symmetric key for every node to the base station. Thus , in Sybil attacks a noxious gadget wrongfully going up against numerous personalities impact large number of network nodes with a specific end goal to deplete its assets or taking delicate data.

Types of Sybil assaults

1. Direct vs. Indirect Communication: In direct communication, Sybil nodes straightforwardly speak with true legitimate node while in Indirect Communication, no real nodes can discuss specifically with the Sybil nodes.
2. Manufactured versus Stolen Identities: In manufacturing, the vindictive node creates number of characters while in stolen, the node hacks an honest node's authentic node ID.

3.5 Wormholes

This kind of attack is imperative and furthermore, it is a perilous attack for WSN kind of deployment. The attacker could record a packet at a solitary area in the system, burrows them to another area, and resends them into the system. The aggressor can replay messages to any piece of the system. In wormhole attacks, malevolent nodes can make a shrouded channel between sensor nodes. A wormhole attack is a vital risk to a wireless sensor network on the grounds that this kind of attack does not entail that a sensor in the system is traded off. See Figure 4.

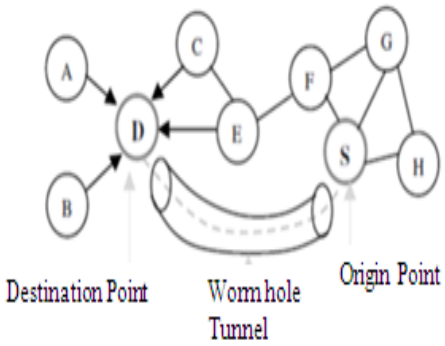

Figure 4. Representation of Worm hole Attack in Network

This kind of attack influences the system layer by constantly hearing and recording information. It can be actualized in the underlying stage when the sensor dispatches to find data [15]. A foe can tunnel all the sensitive messages received into a player node in the system over a low inactivity connection and replay them in another piece of the system. This is normally finished with the coordination of two foe nodes, where the nodes endeavor to downplay their separation from each other, by communicating bundles along an out-of-bound channel accessible just to the attacker. To beat this, the data movement is directed to the base station along a way, which is dependable and topographically shortest or utilize tight time synchronization among the nodes, making the attack situation infeasible in commonsense conditions. The wormhole connection can be set up by numerous kinds, for example, long-range wireless transmission in wireless networks, by using an Ethernet cable, a long-range wireless transmission and an optical connection in a wired medium. Wormhole attack records packets toward one side point in the system and passages them to opposite end-point. These attacks are extreme dangers to MANET and WSN routing protocols. For instance, when a wormhole attack is utilized against an on-request routing convention, for example, AODV/DSR, then all the packets will be transmitted through this malicious path and no other route is found. In the event that the attacker makes the passage sincerely and dependably, then it won't affect the system and furthermore gives the valuable administration in associating the system more proficiently. The attacker can play out the attacks regardless of whether the system correspondence gives privacy and genuineness. A key countermeasure can be integration of the prevention methods into intrusion detection framework. However, it is quite tough to locate the attacker with a software-only approach, since the wormhole nodes send similar packets like their counterpart legitimate nodes. In this case, If single path on-demand routing protocol such as AODV is being deployed in highly dynamic wireless ad hoc scenario, a new route is required to be found in the event of every route break. Each such route discovery demands high overhead and latency. This inefficiency can be overcome with multiple paths route discovery protocol which also addresses the phenomena of all paths breakage in a network. To secure the network against wormhole, a combination of processes, procedures, multipath routing and systems need to be adopted that can ensure confidentiality, authentication, integrity, access control, availability. Few techniques of authentication and integrity mechanism, either by the end-to-end approach or hop-by hop, is useful to provide the accuracy of routing information.

3.6 Hello flood attacks

Hello flood attack has proved to be one of the primary concerns in communication system and it is generally observed in the network layers of WSNs. These attacks are mainly caused by an attacker with high transmission power and that sends or receives the hello packets used for the discovery of neighbor. During these processes, the attacker develops an impression of being a neighbor to other nodes and finds that underlying routing protocol provides disrupting facilities for different types of attacks. Further, the attacker transmits the packets in such a way that large number of nodes are considered as parent node in the WSNs [31]. Figure 5 shows a hello flood attacker broadcasting hello packets with more transmission power than base station. In response to this, a legitimate node has considered the attacker as its neighbor and also an initiator.

In recent years, the research conducted in the field of attacks , ascertains rapid increase in delay while transmitting the message amongst parent node in WSNs. Besides, it has been observed that attacker transmits these hello messages through large number of nodes**.** From this process, the attacker establishes the nodes as the neighbor nodes in the network. Subsequently, considerable amount of energy is dissipated among the nodes while responding to the HELLO message from attackers end , which further leads to confusion state [32].

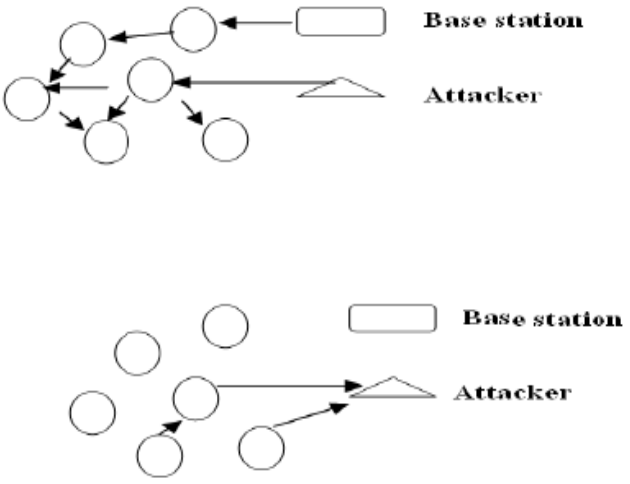

Figure 5. Representation of Hello Flood network

The Hello flood attack recognizes the sensor node, transmits hello message and proclaim itself as their neighbor. Further, any normal neighbor node assumes that the sender/attacker node is in communication range when it receives the hello message and start communicating with that node by providing an entry through its routing table as its neighbor. The communication amongst sensor nodes and base station is provided through the mean of neighbors. The hello message with more power is generated when the attacker tries to capture the legitimate node or develops a fake node in the network and further it produces a dilemma whether the message has been received from neighboring nodes [33]. Moreover, it is observed that hello message has been considered to travel through the shortest path by the nodes from the base station on the basis of assumption that malicious node is the base station and starts communication with the attacker. Through this process, the attacker can gain control over the base station and communication gap raised among the base station and other sensor nodes, which eventually affects the routing process.

The properties of the Hello packet has been categorized into five features and they are as follows,

1. The Hello packet size is less compared to data packet.
2. The tendency of hello packet reaching its destination (receiver) is high compared to data packet in weaker links of the WSNs.
3. The transmission of hello packet is higher at lower bit rate, since basic bit rate is more reliable compared to others.
4. Acknowledgement is not essential while transmitting data in Hello packets.
5. There is no guarantee in bidirectional transmission of hello packets.

Hello packets are capable of providing opportunity for more number of attacks such as flooding, tempering and node capturing, false node replication. These attacks are explained in brief as follows:

Flooding

In this type, a new connection request has been continuously accepted by the neighbor from the attacker for resource capturing. The results observed in legitimate nodes are in terms of severe resource constraints [35].

Tempering and node capturing

Tempering is generally observed in the attacks on the components, which requires alteration in the interior structure of an individual chip. An advisory module can easily recognize it and can be processed for hello flood attack. In this process, the attacker can gain full control over the sensor node through node capture attack. In order to develop node capturing, the attacker should have precise knowledge, efficient equipment with other few resources. The main limitation observed in this technique is complexity in separation or removal of nodes from network [36].

False node replication

In this process, new sensor node has been rooted inside WSNs by an attacker by using the ID of legitimate user. Initially, legitimate ID has been replaced with the false one in the network and replication of this false node along with the support of flood attack can lead to a huge destruction in WSNs. The rate of such damages was predicted to be high and also, the attacker was found to have gained complete access over the network [37].

4.Authenticated Routing Protocols

4.1 Ad-Hoc on Demand Distance Vector Routing (AODV)

The Ad hoc On-Demand Distance Vector (AODV) routing protocol operates with mobile/static sensor nodes for early recognition of the routes and to reach new destination. Here, the nodes are not required to preserve and maintain routes to its destination. The AODV algorithm comprises with features such as autonomous, dynamic, multi hop routing amongst the nodes to establish and maintain route in an ad hoc network. It addresses the issues regarding route breakages and fluctuations in network topology in a well time manner. It is loop free operation and excludes Bellman-Ford "counting to infinity" problem to provide fast convergence rate during the changes in ad hoc network topology, link breakage. Further, the affected set of nodes is identified in order to nullify the routes using the lost link [38].

The demand on various applications of the routing protocol has influenced researchers to modify the basic algorithm and provide better utilization factor in adhoc networking. In this study, various AODV routing protocols have been reviewed, compared to select the effective protocol. Additionally the benefits of ad-hoc frameworks and the present difficulties have been reviewed. Further, this study provides a review on the areas to be enhanced and to understand the capability of the ad-hoc networks. The evaluation parameters such as end to end delay, packet delivery ratio, energy, throughput are often to be considered for analyzing Ad hoc On-demand Distance Vector routing protocol [39] as shown in Figure 6.

Destination	Sequence no	Hop count	Next hop	Time out

Latest trends show that when a specific team goes

Figure 6 Represents the Routing Table structure in AODV

for a gathering or meeting, without a doubt they have a handheld PC or laptop instead of scratch pad. The primary reason behind the fact is that the network information system data assumes a dynamic imperative part in sharing data quicker than with settled base stations. Moreover, it conveys the data related information by means of video or voice, starting with one safeguard colleague to the next through means of portable hand held or wearable remote gadget [40]. The challenges arising in deploying ad hoc wireless networks are,

1. Energy management
2. QoS support
3. MAC protocol

It has been observed from the above study that energy management in handheld devices , can genuinely neglect forwarding packets to Ad hoc mobile environment. Henceforth, the routing traffic on the basis of node energy management is the one way approach to recognize stable route and nodes that are more enduring than others. It's insufficient to consider QoS simply at the system level without considering the fundamental media access control layer. In recent years, the trends in WSNs have been outperformed by QoS approach because of its advantages compared to other approaches. A few ideal models are presented in latest Ad hoc routing methodologies such as reduced time delay, enhanced packet delivery ratio, advanced techniques for path finding and TCP performance to analyze the QoS performance. An adaptable Ad hoc routing protocol can responsively conjure on-demand approaches on the basis of circumstances and communication prerequisites [41]. Additionally, these works are necessary in the future for media access control, and security to understand the capability of Ad hoc networks.

4.2 Optimized Link State Routing (OLSR)

The OLSR commonly acquires the stability of the connection state algorithm into link-state protocol. Individual node recognizes every link in the neighbor nodes and occasionally surges a message containing the entire link connections i.e link State Message [42]. Further, every individual node develops a topology map for the network and freely ascertains the best hop pointing to the destination through shortest path algorithm. Generally, the OLSR routing protocol is an enhanced optimization process to the classical link-state algorithm. The advantages of multipoint relays (MPRs) have been considered as important concept in OSLR [43]. The MPRs mechanism chooses the individual node, which forward transmitted messages during the flooding procedure. This algorithm decreases control packet propagation in the entire network because of the condition that node only selects the subset of the link along with its neighbor MPR selectors. In brief, the packet flooding in the system is considerably decreased because of the fact that exclusive MPRs only create the link state information and communicates the message.

In this way, the MPR nodes may promote just connections among themself and its MPR selectors, thus utilizing partial link-state information for calculating the route.
Only two mobile nodes have been considered in the single hop transmission. A portable mobile node is associated by means of LAN association with Host A, while the other is associated through various LAN associations with Host B. The OLSR routing protocol then spontaneously calculates the link and subsequently creates the routing path. In actuality, every one of the four versatile nodes is utilized in multi hop communication. Single hop experiment also follows similar experimental setup. However, the in-between mobile routers are placed at foreordained areas between two LAN. The chained link between two LANs has been formed by computing the links through OSLR routing protocol and using intermediate routers [44].

4.3 Dynamic Source Routing (DSR)

Dynamic Source Routing protocol is defined as a self-maintaining routing procedure for wireless sensor networks. This protocol can also work with cell phone frameworks and portable systems having up to 200 nodes. A Dynamic Source Routing system can design itself autonomously without the mediation of human overseers. A route on demand can be formed while transmitting the node requests. Self-developed source routing has been utilized at individual intermediate device instead of depending on the routing table. Deciding source routing requires gathering the address of every sensor node between source and destination, during discovery of the route. The captured data is further used by nodes for processing route discovery packets. Moreover, the acquired packets are used in route packets and it comprises with the details regarding the address of the individual device where the packet will traverse [45].
Furthermore, the DSR is considered to be an on demand protocol which is used to monitor and regulate the bandwidth consumption rate by means of control packets in ad hoc wireless networks. Table driven approaches have been considered to do the additional work and updating the table in accordance with changing network conditions. The key comparison amongst the present and on-demand routing protocols is the absence of hello packet transmission, which is used to sense the presence of nearby nodes. The fundamental procedure considered in this protocol is to develop a node's routing database through the process of flooding Route Request packets in the network.
The destination node reacts by replying back with a route reply packet to the source after receiving route request packet. The information regarding traversed route can be obtained through the route reply packet received at the destination node [46].

5 Authenticating Routing Framework

Energy efficient routing protocols have been developed by various authors in order to enhance the life span of Wireless Sensor Networks (WSNs) and balance energy conservation. Different authors reviews along with routing frameworks are as follows,

5.1 Cluster head selection

A priority based load balancing method comprising cluster head selection is used to overcome the limitations arising due to clustering in WSNs [20]. Low Energy Adaptive Clustering Hierarchy (LEACH) technique is deployed to allocate cluster head position amongst member nodes. Later, clustering operation is performed after a particular period of time to return new setup phase and calculate new cluster head. From the experimental study, it has been observed that modified leach protocol comprising cluster head selection provides better results of about 70,000 packets afore the network breakdown, which is much higher compared to other existing techniques. Furthermore, a new clustering approach comprising multi criteria decision making has been developed by author [21] in order to effectively select and manage clusters by considering different criteria. Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) is considered to select the best value and optimize the clusters. From the study, it has been observed the result obtained in terms of number of nodes of 100, initial energy of nodes = 0.5j, shows better performance in terms of lifetime in WSNs compared to other techniques. An enhanced protocol comprising node ranked-LEACH is proposed by author [22] to overcome the limitations such as random process selection in existing techniques and enhance the life span of WSNs. Both past cost and link number amongst nodes is considered to determine the cluster head of the individual cluster and successfully handle shortcomings arises due to extra overhead and high consumption of power. The study on experimental analysis shows that NR-LEACH enhances the lifetime of WSNs compared to other LEACH techniques and provides optimal CH for individual cluster selection. Another research [49], authors proposed HHSRP protocol by developing a mixed hierarchical clustering algorithm that considers greatest value of coordinator node and

fitness value to decide CH. The two key algorithm utilized were mixed hierarchical cluster based routing and hybrid hierarchical secure routing. HHSRP showed the capability of packet transmission based on packet priority and without losing the packets due to any malicious network activity.

5.2 Reputation Mechanism

Reputation Based (RB) security scheme has been developed by author [23] to provide reliability and security to beacon nodes which contain the information of sensor nodes in WSNs. Reputation evaluation model is considered to analyze the performance of the individual beacon node and validated to define the credibility of the beacon node. From the study, it has been observed that RB model successfully increase the accuracy of the WSNs in hostile and untrusted environments. The author specified that in future, this technique can be extended to overcome the issues regarding other malicious attacks. Furthermore, a new model comprising Risk-aware Reputation-based Trust (RaRTrust) technique has been developed in order to analyze the issues regarding insider attacks such as node compromise, traditional security and bypassing [24]. The developed technique has the capability to diagnose and separate malicious and faulty nodes. Further risk evaluation is considered to overcome dramatic node spoiling. The results obtained from the study shows that the proposed model reduces the effect of bad mouthing attack and further stated that recommendations can be aggregated securely when dishonest recommendation is 30% more compared to total recommendation.

5.3 Hash based node authentication algorithm

A new memory based approach called hash table has been considered to evaluate the security and performance of energy consumption in WSNs [25]. In this process, the individual node can be distributed over the entire internet and each node can be controlled using whole resource space and related index information. Finally, different experiments have been conducted by author to evaluate the performance and results shows better performance in terms of energy optimization compared to other techniques. Furthermore, the usage of energy consumption using Hash functions such has MD-5, SHA-1, SHA224, SHA512 has been analyzed by author [26] in authentication nodes of WSNs. The hash functions are represented in the form of optimized codes and processed on virtual computer. It is observed from the study that SHA-224 has outperformed other techniques in terms of real time of 0.1263 sec, user time of 0.0087 sec and system time of 0.0634s. A new authentication scheme comprising Hash based DCHST has been proposed by author [27] to analyze data aggregation problems and energy constraints in WSNs. Distributed pseudo random function has been considered to modify the SHA-1 hash function and deliver collision resistant requirements. It has been observed from the study that combined approach of dynamic clustering along with hash technique increases the security and removes redundancy with improved bandwidth utilization and high data privacy security.

5.4Data replication mechanism

WSN comprises with hundreds of sensor nodes and individual node consists of short-distance wireless links. Because of this wireless links, energy constraint has always been a critical issue. Data replication has proved to be an effective and common way to address these issues and improve data management in WSNs [28]. The advantages of virtual grid concept are used to develop Adjustable Data Replication (ADR) to increase the energy of the popular nodes [29]. The data replication based ADR has been used to increase the life time of the data nodes and WSNs. The data replica nodes are repeatedly built using ADR and near to the query node to provide balance between overhead and energy consumption of the sensor nodes. From the study, the results show that ADR can effectively reduce replica nodes by 60%.and reduced energy consumption by 33% compared to other techniques. Furthermore, a low complexity data replication scheme has been proposed by author [30] to increase the rate of data storage and decrease the probability of data loss. Periodical recycling has been considered to limit the memory usage and greedy distribution storage scheme for data loss prevention. From the study, it has been observed that data dissemination scheme is modeled and simulated and results obtained shows that relative improvement in life time, energy usage and balance amongst data storage and neighbor nodes is observed compared to other techniques.

5.5 Security routing for clustered WSNs

The sensed data should be effectively transmitted among the sensor nodes for detection/prevention of attacks after cluster head selection in WSNs. Secure routing protocol has been developed by author [47] for intrusion detection in clustered wireless sensor networks. An energy prediction model has been developed to ensure the node security and prediction flow model is developed to reduce the attacks arise due to the traffic during routing phase. From the study, it is observed that NS2 simulation tool is used for evaluating the

security of the developed protocol. The results obtained shows better prediction and deliver higher end security against certain routing attacks such as wormholes, Sybil and hello forwarding attacks. A secure routing protocol comprising LEACH and ESPDA, has been developed by author to address the issues regarding secure data aggregation [48]. Several WSNs security requirements such as confidentiality in data, data integrity and source authentication, availability have been considered during the protocol design. The author has compared the developed protocol with its counterpart namely security context, complexity in computation and communication. The results obtained from the study shows better energy aware with high security compared to other existing techniques. Furthermore, an efficient technique on the basis of cluster based hybrid hierarchical secure routing protocol has been developed to analyze the issues arising due to clustering algorithms [49]. An unique technique has been considered for co-ordinator head selection through a combination based cluster algorithm and the co-ordinator head selection has proved to be the highest value of co-ordinator node with fitness value. The description of the packet is received by co-ordinator node through the source node followed by shortest pathway selection on the basis of value generated amongst the intermediate and sensor node. From the study on experimental results, it is observed that HHSRP approach provides better transmission capability between the source to destination without the loss of packet to malicious node.

Table 1. Comparative analysis of the existing techniques

Author	Techniques/Terminologies	Description	Comments
Devi et al., (2017)	Low Energy Adaptive Clustering Hierarchy (LEACH) technique	LEACH technique has been deployed for cluster head selection	Cluster head is used to provide energy balance among all the low priority and high priority nodes. Efficient cluster head selection leads to better energy utilization which tends to higher lifespan of WSNs. It is observed that 70,000 packets have been transferred afore the breakdown of the network
Al Baz et al., (2018)	node ranked-LEACH technique	Advancement of LEACH has been deployed foe cluster head selection and provide balance amongst the nodes	Node rank algorithm which depends on the cost of the path and node link number is used to select the cluster head Different type of LEACH protocol is considered for experimental analysis and result shows that NR LEACH is found to be effective and enhance the lifetime of the system.

Nunoo - Mensah et al., (2015)	HASH functions	Different categories of HASH such as (MD-5, SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512) are considered to evaluate security and energy consumption	Optimized codes have been developed to represent the HASH functions and the same is processed through virtual computer Results show that SHA-224 outperformed other techniques in terms of processing time of around 0.1263 sec
Chen et al., (2016)	Adjustable Data Replication (ADR) Technique	It is used to increase the lifetime of the nodes and WSNs	Results obtained demonstrates that ADR successfully reduces the energy consumption rate by 33% by identifying and neglecting 60% of the duplicated nodes.
Singh et al., (2010)	HELLO flood attack	It is found to be vulnerable type of attack which is used to break the security of WSNs	signal strength and client puzzle method has been used for solving the issues The result obtained shows that it requires less computational energy and power to solve security issues
Ukey et al., (2013)	HELLO flood attack	Recogniti on is achieved through signal strength	Nodes are categorized as stranger and friend on the basis of signal strength If the received reply is within the predefined time, then it is said to be normal node, if it exceeds, then considered it as malicious node Results obtained shows better performance with higher packet delivery ratio compared to AODV technique
Madhavi, S et al., (2013)	HELLO flood attack	Flooding Attack Aware SAODV (FAA-SAODV) technique is deployed to solve the flood attack	Simulation is carried out using NS-2 simulator It is observed that percentage of control overhead is increased compared to SAODV Furthermore, slight improvement has been achieved in terms of PDR ratio and throughput

6.Proposed Method

The methodologies planned for the proposed work are as following:

- Our approach views the WSN network as a square grid and utilizes a grid based clustering method to arrange nodes and to afford an optimized route to the destination, taking advantage of the geometric properties of the grid.
- Design & development of a secure and fast cluster head (CH) selection algorithm. This algorithm will be extended to select a backup CH node, in case the cluster head is not there.
- Design & development of network reputation based system for sensor nodes, in order to authenticate them.

- Design & development of a hash based robust authentication technique that any sensor node will use to provision a set of well reputed neighbours (which are determined by the network reputation based system) with a one-time password and the associated hash function.

6.1 Proposed Secure Routing Framework

The proposed routing protocol consists of couple of functional modules that make it highly efficient to choose the bona fide sensor nodes in network. The high level block diagram of the routing framework is shown in Figure 6. The entire routing engine will be built on the top of already existing routing protocols for WSN, such as aodv ,olsr etc. The lower level interface module will collaborate data from all other modules in order to convey the sensor node validation decision taken by higher level modules.

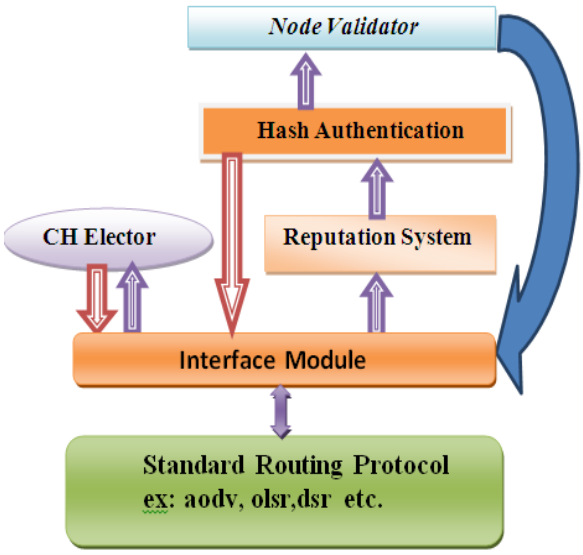

Figure 6: High Level Block Diagram of Routing Framework

7.Discussion

In this research, a wide range of literature overview is presented in terms of wireless sensor network deployment, protocols and security loopholes, which are found to be important aspects and latest trends in the field of communication systems. Different techniques, protocols and algorithms have been considered to address the issues in WSNs such as data clustering and various attacks such as spoofed routing information, selective forwarding, sinkhole, Sybil based attack, wormholes, hello flood attack and acknowledged spoofing is ascertained in this research.

From the aforementioned review as shown in Table 1., it is observed that number of authors have developed different algorithms to address and solve the issues in WSNs. Due to the digitization and increase in the amount of data for communication purpose, considerable amount of work is required to reduce the errors and overcome the attacks. Furthermore, security acts a key constraint and it is to be considered as theprimary factor during the advancement of the communication technologies. From Table. 1 it is shown that HASH based function technique; particularly SHA-224 outperformed other techniques in terms of energy consumption and security with less processing time. The output parameters such as PDR ratio and throughput should be improved to achieve effective and efficient protocol for wireless sensor networks.

The study on routing framework is found to increase the energy consumption rate and enhance the lifespan of the system by providing energy balance between the nodes. From the study, it is observed that HASH based technique is found to be effective in selecting the better cluster head and providing proper communication among the sensor nodes. Furthermore, a study is conducted to address issues arising in Ad hoc mobile environment such as energy management, QoS support and MAC protocol. This study conducted helps to find some research areas and gaps in the field of WSNs in which by developing an efficient algorithm can improve the performance of the system. The future studies comprise with several research topics in the sensor technology field of providing better communication among sensor nodes and issues regarding the security.

8. CONCLUSION

The network vulnerability is more possible with the sensor nodes in an unattended environment. Wireless Sensor networks are gradually increased used by military, health, environmental and commercial applications. Wireless Sensor networks are inherently different from traditional wireless networks as well as ad-hoc wireless networks. Security is a significant aspect for the deployment of Wireless Sensor Networks. In this paper we review the attacks and their taxonomies in wireless sensor networks. Furthermore, an overview has been made to explore the security approach that widely used to handle those attacks. Wireless Sensor Networks challenges are also briefly discussed. In this survey we hopefully motivate the researchers in the futures by using this survey to bring more effective and robust security mechanisms that makes their network more safe.

References

1. Kar, P., Roy, A., Misra, S., & Obaidat, M. S. (2016). On the Effects of Communication Range Shrinkage of Sensor Nodes in Mobile Wireless Sensor Networks Due to Adverse Environmental Conditions. *IEEE Systems Journal*.
2. Bankar, M. S., & Khiani, S. (2016). Securely Data-Gathering Cluster-Based Wireless Sensor Network Design. *International Journal of Engineering Research*, *5*(7), 618-621.
3. Deepa, C., & Latha, B. (2017). HHSRP: a cluster based hybrid hierarchical secure routing protocol for wireless sensor networks. *Cluster Computing*, 1-17.
4. Bera, S., Misra, S., Roy, S. K., & Obaidat, M. S. (2016). Soft-WSN: Software-defined WSN management system for IoT applications. *IEEE Systems Journal*.
5. Rajeswari, K., & Neduncheliyan, S. (2017). Genetic algorithm based fault tolerant clustering in wireless sensor network. *IET Communications*, *11*(12), 1927-1932.
6. Malmskog, S. A., Hoche-Mong, M., & Chang, T. (2011). *U.S. Patent No. 7,979,509*. Washington, DC: U.S. Patent and Trademark Office.
7. Xu, L., Collier, R., & O'Hare, G. M. (2017). A survey of clustering techniques in wsns and consideration of the challenges of applying such to 5g iot scenarios. *IEEE Internet of Things Journal*, *4*(5), 1229-1249.
8. Liu, W. D., Wang, Z. D., Zhang, S., & Wang, Q. Q. (2010). A low power grid-based cluster routing algorithm of wireless sensor networks. In Information technology and applications (IFITA), 2010 international forum on (Vol. 1, pp. 227–229).
9. Jannu, S., & Jana, P. K. (2016). A grid based clustering and routing algorithm for solving hot spot problem in wireless sensor networks. *Wireless Networks*, *22*(6), 1901-1916.
10. Soni, H., & Soni, H. (2015). Comparative Scenario between Grid and Grid based Cluster network in Wireless Sensor Network. *International Journal Of Engineering And Computer Science*, *4*(06).
11. Bara'a, A. A., & Khalil, E. A. (2012). A new evolutionary based routing protocol for clustered heterogeneous wireless sensor networks. *Applied Soft Computing*, *12*(7), 1950-1957.
12. N.Rekha et al, (2015). Wireless Sensor Networks (WSN). *International Journal of Computer Science and Information Technologies*, 6 (4), 3706-3708.
13. Kavitha, T., & Sridharan, D. (2010). Security vulnerabilities in wireless sensor networks: A survey. *Journal of information Assurance and Security*, *5*(1), 31-44.
14. Shabana, K., Fida, N., Khan, F., Jan, S. R., & Rehman, M. U. (2016). Security issues and attacks in Wireless Sensor Networks. *International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE)*, *5*(7), pp-81.
15. Alajmi, N. M., & Elleithy, K. M. (2015). Comparative analysis of selective forwarding attacks over Wireless Sensor Networks. *International Journal of Computer Applications*, *111*(14).
16. Singh, A., & Singh, T. (2016). Review on Detection and Prevention of Sink Hole Attack In network. *Global Journal of Computers & Technology*, *5*(2), 289-292.
17. Vidhya, S., & Sasilatha, T. (2017). Sinkhole Attack Detection in WSN using Pure MD5 Algorithm. *Indian Journal of Science and Technology*, *10*(24).
18. Scholar, M. T. (2017). Review on the various Sybil Attack Detection Techniques in Wireless Sensor Network. *SYBIL*, *164*(1).
19. Upadhyay, S., & Bajpai, A. (2012). Avoiding Wormhole attack in MANET using statistical analysis approach. *International Journal on Cryptography and Information Security*, *2*(1), 15-23.
20. Devi, R., Kumar, A., &Dhawan, V. (2017). A Node Prioritization Based Load Balancing Approach To Improve Cluster Head Selection In Wireless Sensor Network. *architecture*, *3*(02).
21. Hamzeloei, F., &Dermany, M. K. (2016). A TOPSIS based cluster head selection for wireless sensor network. *Procedia Computer Science*, *98*, 8-15.
22. Al-Baz, A., & El-Sayed, A. (2018). A new algorithm for cluster head selection in LEACH protocol for wireless sensor networks. *International Journal of Communication Systems*, *31*(1).
23. He, J., Xu, J., Zhu, X., Zhang, Y., Zhang, T., & Fu, W. (2014). Reputation-based secure sensor localization in wireless sensor networks. *The Scientific World Journal*, *2014*.
24. Labraoui, N., Gueroui, M., &Sekhri, L. (2016). A risk-aware reputation-based trust management in wireless sensor networks. *Wireless Personal Communications*, *87*(3), 1037-1055.

25. Yan, C. (2014, June). Distributed hash table based routing algorithm for wireless sensor networks. In *Intelligent Systems Design and Engineering Applications (ISDEA), 2014 Fifth International Conference on* (pp. 430-433). IEEE.
26. Nunoo-Mensah, H., Boateng, K. O., &Gadze, J. D. (2015). Comparative analysis of energy usage of hash functions in secured wireless sensor networks. *International Journal of Computer Applications*, *109*(11).
27. Poonguzhali, P. K., &Moorthy, N. A. (2017). Design of a Dynamic Clustering With Secured Hashing Technique in Wireless Sensor Network. *Asian Journal of Applied Science and Technology (AJAST)*, *1*(4), 28-33.
28. Hamrouni, T., Slimani, S., &Charrada, F. B. (2015). A critical survey of data grid replication strategies based on data mining techniques. *Procedia Computer Science*, *51*, 2779-2788.
29. Chen, T. S., Wang, N. C., & Wu, J. S. (2016). An efficient adjustable grid-based data replication scheme for wireless sensor networks. *Ad Hoc Networks*, *36*, 203-213.
30. Ekbatanifard, G. (2017). An energy efficient data dissemination scheme for distributed storage in the internet of things. *Computer and Knowledge Engineering*, *1*(2), 1-8.
31. Singh, V. P., Jain, S., & Singhai, J. (2010). Hello flood attack and its countermeasures in wireless sensor networks. *IJCSI International Journal of Computer Science Issues*, *7*(11), 23-27.
32. Hamid, M. A., Rashid, M. O., & Hong, C. S. (2006). Routing security in sensor network: Hello flood attack and defense. *IEEE ICNEWS*, 2-4.
33. Singh, V. P., Ukey, A. S. A., & Jain, S. (2013). Signal strength based hello flood attack detection and prevention in wireless sensor networks. *International Journal of Computer Applications*, *62*(15).
34. Singla, A., & Sachdeva, R. (2013). Review on security issues and attacks in wireless sensor networks. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(4).
35. Madhavi, S., & Duraiswamy, K. (2013). Flooding attack aware secure AODV. *Journal of computer science*, *9*(1), 105-113.
36. Ghildiyal, S., Mishra, A. K., Gupta, A., & Garg, N. (2014). Analysis of denial of service (dos) attacks in wireless sensor networks. *IJRET: International Journal of Research in Engineering and Technology*, *3*, 2319-1163.
37. Rathod, V., & Mehta, M. (2011). Security in wireless sensor network: a survey. *Ganpat university journal of engineering & technology*, *1*(1), 35-44.
38. Zapata, M. G. (2002). Secure ad hoc on-demand distance vector routing. *ACM SIGMOBILE Mobile Computing and Communications Review*, *6*(3), 106-107.
39. Marina, M. K., & Das, S. R. (2006). Ad hoc on-demand multipath distance vector routing. *Wireless communications and mobile computing*, *6*(7), 969-988.
40. Royer, E. M., & Toh, C. K. (1999). A review of current routing protocols for ad hoc mobile wireless networks. *IEEE personal communications*, *6*(2), 46-55.
41. Belding-Royer, E. M., & Perkins, C. E. (2003). Evolution and future directions of the ad hoc on-demand distance-vector routing protocol. *Ad Hoc Networks*, *1*(1), 125-150.
42. Clausen, T., & Jacquet, P. (2003). *Optimized link state routing protocol (OLSR)* (No. RFC 3626).
43. Clausen, T., & Jacquet, P. (2003). RFC 3626: Optimized link state routing protocol (OLSR). *IETF*, *October*, *4*.
44. Yi, J., Adnane, A., David, S., & Parrein, B. (2011). Multipath optimized link state routing for mobile ad hoc networks. *Ad hoc networks*, *9*(1), 28-47.
45. Ghuman, S. S. (2016). Dynamic Source Routing (DSR) Protocol in Wireless Networks.
46. Awerbuch, B., Mishra, A., & Hopkins, J. (2016). Dynamic Source Routing (DSR) Protocol. johns hopkins university, US.
47. Zhenghong, X., &Zhigang, C. (2010, July). A secure routing protocol with intrusion detection for clustering wireless sensor networks. In *Information Technology and Applications (IFITA), 2010 International Forum on* (Vol. 1, pp. 230-233). IEEE.
48. Rahayu, T. M., Lee, S. G., & Lee, H. J. (2015). A secure routing protocol for wireless sensor networks considering secure data aggregation. *Sensors*, *15*(7), 15127-15158.
49. Deepa, C., &Latha, B. (2017). HHSRP: a cluster based hybrid hierarchical secure routing protocol for wireless sensor networks. *Cluster Computing*, 1-17.

Journal of AL-Qadisiyah for computer science and mathematics Vol.10 No.3 Year 2018
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

طرق بروتوكولات التوجيه الآمنة في شبكات الاستشعار اللاسلكية

وليد خالد حسين
جامعة تكنلوجيا المعلومات
معهد الدراسات العليا

شيماء حميد شاكر
الجامعة التكنلوجية
قسم علوم الحاسبات

المستخلص:
تنظر شبكات المستشعرات اللاسلكية (WSN) في تكنولوجيا ناشئة تم استخدامها بشكل كبير في الحالات الحرجة مثل ساحات المعارك والتطبيقات التجارية مثل مراقبة حركة المرور، ومباني البناء، والبيوت الذكية والرصد والعديد من السيناريوهات الأخرى. يعد الأمان أحد التحديات الرئيسية التي تواجه شبكات المستشعرات اللاسلكية في هذه الأيام. في حين أن البيئة غير المراقبة تجعل نشر عُقد أجهزة الاستشعار في الشبكات أكثر عرضة للهجمات المحتملة، فإن القيود المفروضة على الطاقة المتوفرة والذاكرة لعقد أجهزة الاستشعار تجعل الحلول التقليدية للأمان غير قابلة للتطبيق. تجعل تكنولوجيا الاستشعار المدمجة مع طاقة المعالجة والاتصالات اللاسلكية من المربح للاستغلال بكمية كبيرة في المستقبل. تكنولوجيا الاتصالات اللاسلكية أيضا الحصول على أنواع مختلفة من التهديدات الأمنية. تناقش هذه الورقة مجموعة واسعة من الهجمات في WSN وآليات تصنيفها وأليات الحماية المختلفة المتاحة للتعامل معها بما في ذلك التحديات التي تواجهها.