Integrated Intelligent Research(IIR)

International Journal of Communication and Networking System
Volume: 05 Issue: 02 December 2016,Pages No.105-112
ISSN: 2278-2427

A Survey on Secure and Power Aware Routing Protocols in Wireless Sensor Networks

R. Dharani, M.V.Srinath
Research scholar, Bharathidasan University, Trichy, India
Director MCA, STET Women's college, Mannargudi, India
Email: dharaninagavalli@gmail.com, sri_induja@rediffmail.com

Abstract - The development of wireless sensors and the advances in Wireless Sensor Networks (WSNs) have exposed new scenarios where sensors can be quickly deployed without any existing infrastructure. It is very helpful in many applications such as military applications, emergency rescue, environmental control, health monitoring etc. Though, WSN faces many challenges, these networks are severely susceptible to network attackers, because any sensor within the frequency range may get access to the network. Hence, there is a need for security algorithms and awareness of the network challenges. Due to the lack of security measure, the attackers mislead the entire network operations and waste the network resources. It results in poor network lifetime, computational resources, memory, etc. Hence, a secure and power aware techniques are necessary to improve the network lifetime. This survey presents the various security and power aware routing algorithms for WSNs which helps to recognize the scope and nature of the protocol. The aim of this paper is to provide the extensive analysis of the various security and power aware routing protocols. The comparison of security protocols includes the cipher type and the attack types it protects. The comparison of power aware routing includes the extensive analysis of protocol classification, power usage, data aggregation, scalability, data delivery model and overhead.

Keywords- Attackers; Network Lifetime; Network Resources; Power Aware Techniques; Security; and Wireless Sensor Networks (WSNs).

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are composed of small sensing devices called sensors. It communicates through wireless following an ad hoc formation. The sensor nodes are located in a medium such that they can communicate with one another and also they can share their sensed data. Usually, these sensor nodes depend on the broadcast type of communication. These nodes are considered by low computational capabilities, limited energy, and limited amount of memory. WSNs were found to have used in fascinating applications like surveillance applications, forest fire detection, moisture control in agricultural areas, building computerization and security applications. Moreover, WSNs can also be used in fire detection in forests and environment monitoring applications. Security and power management are the major issues in the WSNs. The combination of security and power aware techniques are necessary to successfully accomplish the routing in WSNs.

Some of the applications of WSNs such as military surveillance, space exploration, disaster detection and relief, etc., necessitate a secure communication network for data transfer from the sensor to the Base Station (BS). Without the use of security mechanisms, such applications may consequence in undesirable significances. For example, in the disaster detection and relief application, an attacker node may forward false information such as bogus disaster warning producing massive financial loss as a result of deployment of disaster equipment's and larger scale evacuation.The constraint of such applications requires the security as one of the major concerns of network scheme. The security attacks may be protected with the help of strong cryptographic mechanism. However, the cryptographic mechanisms are established for both ad-hoc networks and for traditional wired networks. It cannot be utilized for the WSNs due to the following reasons:

- The Public-key algorithms are not right for WSN because of the high computational complexity and huge code size linked with such algorithms.
- The execution of cryptographic algorithms necessitates more power, memory, and processing time. But the nodes have only limited resources; hence it is essential to use an algorithm which utilizes only limited resources.
- Sensor nodes are habitually installed in a hostile environment. In this situation, the sensors are open to the physical attack.

These reasons paid consideration for designing the security algorithms for WSNs. The attacks can be classified into two types: 1. Internal and 2. External attacks. Figure. 1 depicts the classification of attacks.

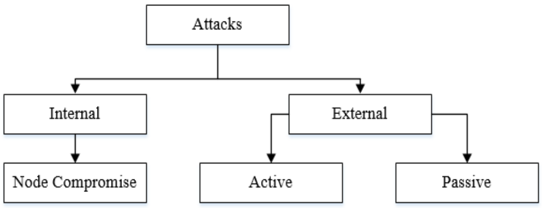

Figure 1. Classification of Attacks

Node Compromise is the chief attack in WSN which leads to the internal attacks. Internal attack is established to disable nodes. The compromised nodes actively pursue to paralyze or interrupt the network. Adversary nodes capture the sensor nodes and reprogram their functionalities. But, it is not easy to automatically reprogram the sensor, it would be done by manually. In some applications, the deployment location makes it problematic or even impossible for adversaries to capture the sensors. In external attack, the attacker node is not a legal member of the sensor network. It is categorized as active attacks and passive attacks. Active attack interrupts the network functionality by announcing Denial-of Service (DoS) attacks, like power exhaustion and jamming. Passive attack includes an illegal listening to the routing packets. It can be avoided with the help of encryption security algorithms. Integrity and authentication will eliminate most of the active attacks excluding for jamming. Jamming can be protected by various forms of frequency hopping or spread-spectrum communication. It is essential to offer the security algorithm in order to provide data confidentiality, data integrity, data authenticity, data freshness and availability.

There are several matters accountable for power excess in sensor nodes in WSNs. They are given as below:

a) Idle listening: Every time a sensor node remains to listen or sense to a channel, it waits for the information received from the other sensor nodes, it pays to the major cause of energy wastage. At this time, the sensor nodes only listen but do not transfer/receive.
b) Packet collision: Whenever two nodes attempt to forward the data packets to the same node, then there is a frequent option of collision among these packets. If the collision occurs, then the packets are discarded and it results to energy wastage because these collision packets requisite to be retransmitted again. This process consumes energy.
c) Overhearing: Overhearing occurs due to the cause of energy wastage in sensor network. It happens once a node by itself becomes an intended receiver node and remains listening to the channel and also overhears a packet not destined for this node. This node takes itself as a possible receiver node, but in reality the packet is addressed to some other sensor node.
d) Over emitting: It occurs when a transmitter node concerned in forwarding the data packets to the receiver node, which essentially is not prepared for receiving those packets, and hence those packets are lost and the packet should be retransmitted. The retransmission process consumes energy.
e) Control overheads: The control packets are forwarded by one sensor to another to indicate their presence. The presence of handshaking message and control overheads may result to energy consumption in sensor network.

In order to prevent the network from energy wastage issues, the routing protocol should be incorporated with the power aware mechanisms. Also, security measures are appended on the network to maintain data confidentiality, data integrity, data authenticity, data freshness and availability. This survey provides the various algorithms for security and power aware routing in WSNs.

The paper is organized as follows: Section 2 describes the various security routing algorithms in WSNs. Section 3 provides the various power aware routing algorithms in WSNs. Finally, the paper is concluded in section 4.

II. Secure Routing Algorithms in WSNs

Most of the routing protocols for WSN do not support the security they are mainly concerned about the data transfer [7].The secure routing protocols for sensor networks are broadly classified into three types. They are:

1. Secure Hierarchical Routing Protocol
2. Secure Multipath Routing Protocol
3. Secure Geographical Routing Protocol

There are several protocols that have been proposed in the past few years under this classification. This section discusses about the three categories of secure routing protocols in WSNs.

A) *Secure Hierarchical Routing Protocol*

Yin and Madria [8] offered a Hierarchical Secure Routing Protocol Against Black Hole Attacks (HSRBH) for WSN. Black hole attack is a severe type of attack which can be easily executed against routing in sensor networks. This protocol utilizes the symmetric key cryptography to identify the safest route against black hole attack. This protocol uses the randomized data acknowledgement strategy to identify the attack. Here, the source node randomly forwards the control packets to the destination node to forward the acknowledgement. This message comprises of shared key between source nodes. The node can accept the acknowledgement and verification prospers for secure route discovery. Otherwise, it is considered as a black hole attack and moves the node address into the blacklist. Once the secure route discovery process gets completed, each node on the route has constructed the routing table. The table contains the next hop address on the route to the destination hole.

Du et al [9] discusses a Two Tier Secure Routing (TTSR) protocol for heterogeneous sensor networks. This protocol has two heterogeneous network models. They are High-end Sensor (H-Sensor) and Low-end Sensor (L-Sensor). H-Sensors are tamper resistance which can’t be easily compromised. Also, TTSR has two tier routing scheme called intra-cluster routing and inter-cluster routing. Intra-cluster routing is the routing executed within the cluster and inter-cluster routing is the routing across the cluster. In intra-cluster routing, the packets are sent to the cluster head by constructing the minimum spanning tree or shortest path. Whereas for inter-cluster routing, the cluster head eliminates the redundant data and forwards the data to the BS after verifying the key and location information. This protocol eliminates the Sybil attack with the help of authentication among the nodes to guarantee that one node cannot pretend to be another node. Moreover, this protocol defends against sink hole and wormhole attacks. Because, datas are transferred to BS with the help of H-Sensor and relay cells. Hence, the attacker cannot modify the route in TTSR. It prevents the flood attack, as the L-Sensor utilizes the two-way handshake protocol to initiate the neighbor relationship.

Kausar et al [10] proposed a key management and secure routing in heterogeneous sensor networks. Here, the key management approach follows the random key pre-distribution into order to attain better security and performance. During key distribution phase, all the keys in the key pool are allocated to H-Sensor because it is more powerful and tamper resistant to L-Sensor. It minimizes the storage requirements while facilitating the entire network connectivity. Authentication is used to ensure the protocol against Sybil attack. Message Authentication Code (MAC) is calculated among the nodes with the help of shared pair wise key. Here, sink hole and wormhole attacks are not possible because attacker node cannot route the packet in relay cells among H-Sensor and BS. Since H-Sensors are tamper resistant it is safeguarded from the node compromise attack, but L-Sensors can be compromised. To overcome this issue, the packet is included with the unique ID and compromised node ID is also attached. Hence, the attacker node cannot receive the data.

Madria and Yin[11] implemented a Secure Routing protocol against wormhole attacks (SeRWA). Wormhole attack is very hard to identify since it accepts the data from one node and forwards the data to the destination using another node without compromising the nodes. This protocol has four phases: neighbor discovery process, initial route discovery, data distribution and wormhole attack identification and secure route discovery. The destination node broadcast the packet and node which receives the packet is marked as the parent and rebroadcast the packet. It is repeated until the network topology is created.

Lee and Choi [12] presented a Secure Alternate Path Routing in Sensor Network (SeRINS). This protocol composed of three phases: an alternate path scheme, neighbor report system and neighbor authentication. During alternate path phase, every node maintains multiple parents. The alternate path is created by the BS by forwarding the sequence number. It is established with the help of one way hash function and hop count. The details are broadcasted to the next level of sensors which verifies the hop count and a sequence number. If the count is equal or lesser than the parent node, then each node record the node forwarding the route update as the genuine parent node. Otherwise, it is eliminated. In neighbor report system, the alternate path facilitates the network robust for compromised nodes. The nodes which are compromised are forge itself with the help of hop count. During neighbor authentication, the compromised node forges its identity and forward some other sensor as forge node. It creates a delay for broadcasting the packet and it also buffers the data. The buffering and information delay can be identified with the help of authentication.

Yin and Madria [13] suggested a Secure Routing Protocol (SecRout) for sensor networks. This protocol uses two levels of security measure to forward the data from source to destination. It utilizes the symmetric key cryptography to securely forward the data. During the first level of routing, the source node transmit the data to the cluster head with the help of cluster key. The cluster key uses the sensor cache to save the information about the previous hop and next hop. The cluster head forwards the data to the destination node with the help of shared key. This protocol can easily recognize the selective forwarding and compromised node attack.

Zhang et al [14] proposed a Random pair key for Low Energy Adaptive Clustering Hierarchy (RLEACH) protocol for sensor network. LEACH protocol is severely affected from attacks and they are not secure. Hence, RLEACH is introduced, which uses the Random Pairwise Key (RPK) for security. RPH manages the key pool, it comprises of L different key chains. The key chain is established with the help of one has function by public seed and key. It prevents the network from network layer attacks like selective forwarding attack. This protocol uses the node-to-node authenticating. Hence, Sybil attack and hello flood attacks are not possible in this protocol.

B) *Secure Multipath Routing Protocol*

Tang and Li [15] proposed a Secure-Sensor Protocol for Information via Negotiation (S-SPIN). SPIN protocol does not include any security algorithms for data transferring. It is vulnerable to many attacks. Hence, the S-SPIN protocol is introduced with security measures. This protocol is a three stage protocol where the node uses three categories of messages called advertise (ADV), request (REQ) and data message. When a sensor node receives a new data, then it sends ADV message to its neighbor nodes. The interested nodes will forward the REQ message to retrieve the data. ADV and REQ messages are protected using a MAC. It ensure secure data transfer among the sensor nodes. S-SPIN protocol works more efficiently and consumes lesser energy and bandwidth. It forwards the metadata to the neighbors before forwarding the original data.

Zhou et al [16] presented an Intrusion Tolerant Secure Routing Protocol (ITSRP) with key exchange for WSN. This protocol combines the energy factor and authenticated key exchange into the secure routing algorithm. It manages the damages occurred by attackers which has compromised the sensor nodes. This protocol uses the local routing table for routing the packets. The table contains unique ID, tag#, energy, lifetime, ancestor and successor. ITSRP has three phases: path discovery, route establishment and secure data transfer. When a source node needs to forward a message to destination, it has neither shared session key nor route path. The source node transmits packets with a unique tag and set the ancestor value as ‘0’. It broadcasts the message to the entire network within the range. The nodes are accepting the message and verifying the destination address. If the node is not the given destination, then it updates the routing table and send the packet. If it is recognized as the destination, then it recovers the packet with the distributed key and update the routing table. In the last phase, the node transfer the data using session key. The session key is created by the ITSRP protocol, hence it is more secure.

Gui et al [17] implemented a Secure routing and Aggregation protocol with Low Energy cost for sensor networks (STAPLE). This protocol uses the one-way hash function and multipath routing to accomplish secure data transfer. This protocol is composed of three phases. They are initialization phase, data transfer and filtering and source authentication sink. During the initialization phase, the destination node broadcast the hello message to the sensor nodes. The source node forwards the acknowledgement message to the destination with source ID. The destination node calculates its key using one-way hash function. A destination node removes the random number from memory to eliminate the unwanted storage space. During data transfer and filtering, the source node forwards the data to its parent node and then transfers the data to the destination node using hop by hop fashion. In the last phase, the protocol authenticates the source node identity and data integrity.

Cheng et al [18] introduced a Curve Based Secure Routing algorithm for sensor network. This protocol uses the Curve based Greedy Routing (CBGR) to generate the curve for data transmission. All the sensor nodes are broadcast the packet with Time to Live (TTL), the position of the node and sequence number. After receiving this message, the protocol generates the neighbor table and each sensor will have the sharing key with its direct neighbor node. The flooding method is used by the destination to broadcast the position and required data. The destination node uses the master key to estimate the length of the key and encrypts the message and then broadcast it. This protocol creates B-Spline curve to transfer the data as it needs lesser computation complexity which consumes less energy. This protocol is resilient against selective forwarding attack. Moreover, CBGR does not manage all the connections between source to destination, hence it prevent the network from hello flooding attack.

Jiang and Zhao [19] presented a Secure Routing protocol with Malicious Node detecting and diagnosing for WSNs. This method uses the μ- Timed Efficient Stream Loss-tolerant Authentication. Most of the secure routing approaches consider the flat network. But this approach uses the cluster network and uses the simplest way to identify the malicious nodes. For example, if a node ‘m’ forwards the data and saves the data in the buffer and wait for receiving the acknowledgment. If the acknowledgment message is not received, then it is recognized as the malicious node. This process gets repeated until the data reaches the destination node. Wen et al [20] proposed a segment Transmission Secure Routing Protocol for WSNs. Here, the source node identifies the neighbor nodes and decides some of the sensors as relay nodes. The source node splits the data into small segment based on the code type and length, number of relay node and gives a unique identification number for each segment. The source encrypts the message with the help of shared key and appends the code which verify the data automatically. The source node appends the message header for all the segmented data. The header includes message ID, sensor ID, number of segments and index. This protocol uses the light weighted cryptography for encryption. Hence, this protocol consumes lesser energy for data transmission.

C) *Secure Geographical Routing Protocol*

Yao and Zheng [21] introduced a Secure Routing Scheme based on Multi-objective optimization for WSN. This protocol uses the node location information and trust technology to generate the route. But, this protocol implements for static network only. The secure route is generated based on the trust value, number of hops to the destination node and the remaining energy. Authentication and encryption are used between the neighbor nodes for data exchange which guarantees data integrity and confidentiality. This protocol is composed of three main phases: initialization phase, routing discovery phase and acknowledgement phase. Initialization phase is divided into online and offline. During the online phase, every node estimates its hops to every destination and formulates its neighbor list based on their distance. If the distance between the cell center and the center of its one neighbor cell is greater, then it recognized as the malicious node and moved into the blacklist. If the source node accepts the acknowledgment message from the neighbor node, then the packet can be forwarded successfully. Yin et al [22] proposed a Secure Routing on the Diameter (SRD) which provide efficient and scalable data delivery from source to destination node. SRD uses the token strategy in order to provide security to huge sensor network. Hence, the energy taken for computation is lesser for calculation. Ticket server is used to establish the route in diameter with the help of pre-loaded token. The server encrypts the data with the help of its private key. During data transmission, the nodes authenticate each other with the help of the private key.

III. Performance Analysis

The need for security algorithm is to eliminate the unauthorized access from the attackers and to eliminate the unwanted power resources. The packer are secured with the help of several authentication algorithms and also they are resilience against various attacks. Table I provides the different cipher types and attacks which it manages.

Table I. Comparison of Various Security Algorithms

Protocol Name	Cipher Type			Attack Types					
	Symmetric	***Asymmetric***	***Other***	***Spoofed, altered***	***Forwarding***	***Sinkhole***	***Sybil***	***Wormhole***	***Hello flood***
Secure Hierarchical Routing Protocol									
HSRBH [8]	✓					✓		✓	
TTSR [9]	✓				✓	✓	✓	✓	✓
Key management and secure routing [10]	✓				✓	✓	✓	✓	
SeRWA [11]	✓					✓		✓	
SeRINS [12]				✓	✓	✓			
SecRout [13]	✓			✓	✓				
RLEACH[14]							✓		✓
Secure Multipath Routing									
S-SPIN [15]	✓								
ITSRP [16]	✓					✓		✓	
STAPLE[17]	✓				✓		✓		
CBGR [18]			✓		✓				✓
Secure routing with malicious node [19]			✓	✓			✓		
Segment transmission secure routing [20]	✓								• ✓
Secure Geographical Routing									
Secure routing based on multi objective optimization [21]	✓			✓	✓				
SRD [22]			✓				✓		✓

Table 1 illustrates the types of cipher type for each protocol and the attack types it defends. The above mentioned protocols are implemented to protect the sensor network against various attacks such as spoofed/altered, forwarding, sinkhole, Sybil, wormhole and hello flood. The differentiations of these protocols are also listed in the table 1.

IV. POWER AWARE ROUTING ALGORITHMS IN WSNS

Vidhyapriya and Vanathi [23] presented an Energy Aware Routing (EAR) for WSN. This protocol facilitates a reliable transmission situation with minimum energy consumption. EAR effectively uses the available energy and received signal strength among the nodes to find the optimal route to the sink node. EAR includes three phases: neighbor discovery, route reply and reliable transmission. When the destination node receives an interest, then the node establishes a neighbor discovery phase. A message is broadcasted through the network until it obtains the source node. The broadcast message includes the source address, sequence number and hop count to categorize the message is from the same source or from the different source. Also, the list contains the received signal strength, required energy and destination address. Then, it forwards the reply message through the neighbor nodes. The neighbor discovery process generates a neighbor group list, which includes the address of all the nodes. Once the routes are generated between the source and destination, they are saved in the routing table. It stores the information about the route which can be used to forward the data packets and check the validity of every table record. The routing table includes the destination address, next hop, hop count, sequence number and lifetime. EAR offers reliable packet delivery for data transmission. Here, data is saved on the sender side until an acknowledgement message is received from the receiver node. If no acknowledgement is received, then the data will be forwarded to the source node for retransmission.

Gill et al [24] suggested a Low Energy Adaptive Clustering Hierarchy (LEACH) protocol for WSN. LEACH maximizes the lifetime of sensor networks by minimizing the energy required to generate and manage cluster heads. This protocol includes several rounds with two major phases.

1. Setup phase and
2. Steady phase

The setup phase has three steps: 1. Cluster head advertisement, 2. Cluster setup and 3. Formation of transmission schedule. In the first step, the cluster head forwards the advertisement packet to negotiate the cluster nodes which have become the head. The head is selected based on the threshold value. The node is selected as the head, if the value is lesser than the threshold. In the cluster setup step, the cluster nodes receive the cluster head advertisement message and forwards the join request to the cluster head by informing that they are the member nodes of the cluster. The member nodes preserve the energy by switch off the transmitter and switch on only when they are required to forward the data to cluster head, In the last step, each cluster head formulates the transmission schedule for the member of their clusters. Hence, TDMA schedule is used based on the number of members in the cluster.

Then, every node forwards their data in the allocated time slot.During steady phase, the member nodes forwards the data to the cluster head. The member nodes only communicate with the cluster head through single hop transmission. The cluster head collects all the gathered data and forwards to the BS. It helps to reduce the network traffic. Moreover, single hop transmission saves significant energy.

Roychowdhury and Patra [25] proposed a Geographic Adaptive Fidelity (GAF) protocol. GAF optimizes the performance of WSN by identifying the equivalent nodes on behalf of the packet packets. Every node uses the location information with the help of GPS to link itself with the virtual grid. The entire network is divided into several square grids. The node which has the highest residual energy is selected as the master for each grid. For each grid, one node (master) will be elected to stay active for a particular period of time and then it will go to sleep. This node takes the responsibility to monitor and report the data to the destination. Other nodes are safely put to the sleep mode. GAF uses three states for routing the packets.

1. Discovery: estimate the neighbor nodes in the grid.
2. Active: negotiating the participation for routing and
3. Sleep: switch off the nodes to conserve energy.

The sleeping neighbor nodes manage their sleeping time to preserve the routing fidelity. GAF is highly scalable and utilizes limited power usage. Kour and Sharma [26] introduced a Hybrid Energy Efficient Distributed (HEED) protocol for WSN. It is a clustering protocol and each cluster is elected with the cluster head. HEED uses the residual energy as the primary parameter and the other network topology features such as node distance and degree to neighbors are used as the subordinate parameters. Cluster heads are elected based on the residual energy among the nodes. Intra cluster communication takes as the subordinate parameter to break the ties. A tie means a node may fall within one or more than one cluster head. The intra cluster communication cost is the function of two factors:

1. Cluster characteristics such as cluster size and
2. Whether or not power levels are allowable for intra cluster data communication. If the power level for cluster communication is assigned to all the nodes, then the cost is proportional to node degree.

Each node executes neighbor discovery and send it cost to the identified neighbor nodes. Every node assigns the probability of the chance of becoming a cluster head. The value of CH prob is not permitted to fall below the threshold value. Lindsey and Raghavendra [27] presented a Power Efficient Gathering in Sensor Information System (PEGASIS). The chief idea of this protocol is for every node is to transmit and receive to close neighbors. This approach helps to evenly distribute the load among the sensor nodes. The nodes are organized to create a chain, which is implemented based on the greedy algorithm starting from any node. On the other hand, BS also estimates the chain and advertise to all the sensor nodes. To guarantee that all the sensor nodes have close neighbors is complex, which is also same to the traveling salesman problem. Hence, greedy approach is used to overcome this problem and construct the chains before the initial level of communication. The chain is constructed with the starting node which is nearest to the BS. Because, as per the greedy algorithm, the nearest distance will gradually increase since nodes in the chain cannot be reconsidered. This protocol executes data merging at every node except the last node in the chain. All the node fuses its neighbor packet with its own packet to create a distinct packet of the same length. Then, the single packet is forwarded to the neighbor nodes. It balances the energy depletion problem and preserves robustness among the sensor nodes.

Li et al [28] presented a Hierarchical Power Aware Routing (HPAR) in sensor networks. HPAR consider the path with minimum energy than to use the path with the highest residual energy nodes. It aims to fix a balance between reducing the energy conservation among the nodes. Hence, Dijkstra algorithm is utilized to sort the path with minimum energy. Here, the entire network is divided into zones. The path towards the zones is decided with the help of maximum power value among all the routes. This route is termed as max-min path. Sadagopan et al [29] discussed an Active Query Forwarding in Sensor Networks (ACQUIRE). The basic idea of this protocol is to consider the query as an active element, which is forwarded through the entire network. ACQUIRE has the look ahead parameter in the following way: an intermediate nodes which manage the active query use information from all sensors within the d hops to partially solve the query. After the query is fully solved, then the complete response message is forwarded to the querying node. A mathematical model scheme is proposed to estimate the energy associated with the protocol.

Manjeshwar and Agarwal [30] proposed a Threshold Sensitive Energy Efficient Sensor Network protocol (TEEN) for re-active networks. A node continuously monitors the network and move to the transmission mode when the particular threshold is attained. Here, two kinds of thresholds are used. One is hard threshold and the other one is soft threshold. When the hard threshold is attained, the nodes regather the data and move to the transmission mode and forward the sensed data to the cluster head. The major demerit of this protocol is that of the broadcasted threshold is not received, then the sensed packet will not be transmitted. The same authors [31] introduced Adaptive TEEN (APTEEN) protocol for WSN. APTEEN is adaptive in nature which is based on the user requirement and application type. Here, the values of threshold are varied based on the application type and requirement. The nodes keep on sensing the network and only the hard threshold nodes can move to the transmission mode. Moreover, the nodes can also pass on the packet when the soft threshold is attained. He et al [32] proposed a Stateless Protocol (SPEED) for real time communication in sensor networks. This protocol uses the geographical location to make the routing choices. It maintains the anticipated data delivery speed across sensor networks by locally managing the packets and diverting traffic at the network layer. It uses a single packet format and contains the following fields: TTL, packet type, destination, global_ID and payload. Every node maintains a neighbor table to save the beacon information. The neighbor table has position, expire time, send to delay and neighbor ID. The integration of network layer and MAC enhances the data delivery and facilitate better response to voids and congestion.

Performance Analysis: Table II presents the comparison of power aware routing protocols in WSNs. It provides the classification type of the protocol, power usage (Low, Medium, Limited, Maximum and High), data aggregation (Yes/No), Scalability (Good/Limited), data delivery model and overhead (Low, High, Moderate, and Good).

Table II. Comparison of Power Aware Routing Protocols

Routing protocol	**Classification**	**Power Usage**	**Data Aggregation**	**Scalability**	**Data Delivery Model**	**Overhead**
EAR [23]	Flat	Low	No	Limited	Continuously	Low
LEACH [24]	Hierarchical/ destination	High	Yes	Good	Cluster head	High
HEED [26]	Hierarchical	Low	Yes	Good	Hybrid	Low
HPAR [28]	Hierarchical	Low	No	Good	Demand driven	Less
TEEN [30]	Hierarchical	High	Yes	Good	Active threshold	High
APTEEN [31]	Hierarchical	High	Yes	Good	Hard and soft threshold	High
PEGASIS [27]	Hierarchical	Maximum	No	Good	Chains based	Good
GAF [25]	Hierarchical/ Location	Limited	No	Good	Virtual grid	Moderate
ACQUIRE [29]	Flat/data centric	Low	Yes	Limited	Complex query	Low
SPEED [32]	Location/data centric	Low	No	Limited	Geographic	Low
Directed diffusion	Flat/destination	Limited	Yes	Limited	Demand driven	Low
SAR	Data centric	High	Yes	Limited	Continuously	High
Rumor routing	Flat	Low	Yes	Good	Demand driven	Low

Table 2 provides the extensive analysis and comparison of various power aware routing protocols. The table provides the set of following properties for comparative analysis. It includes protocol classification, power usage, data aggregation, scalability, data delivery model and its overhead. It helps to realize the nature and scope of the above mentioned protocols.

V. CONCLUSION

Routing in sensor networks has concerned a lot of attention in the past few decades and introduced a unique challenges when compared to the existing data routing in wired networks. This paper summarizes the various security and power aware routing algorithms for WSNs. The major three categories of security algorithms and power aware algorithms are discussed in this paper. The comparative results of the various security algorithms and power aware routing algorithms are also provided. The comparative table for security protocol provides the cipher type of the protocol and the type of attack it defends. The comparative table for power aware protocols includes protocol classification, power usage, data aggregation, scalability, data delivery model and its overhead. From this survey, the reader can easily recognize the scope and nature of the security and power aware protocols. In order to provide successful data delivery for sensor network, the routing algorithm should be incorporated with the security and power aware mechanisms. It is noted that substantial reduction in energy depletion of nodes in a WSN can be accomplished with the help of security and power aware algorithms. In the future, we planned to design an efficient power management and security technique for WSNs.

References

[1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Computer networks, vol. 52, pp. 2292-2330, 2008.

[2] S. P. Singh and S. Sharma, "A survey on cluster based routing protocols in wireless sensor networks," Procedia computer science, vol. 45, pp. 687-695, 2015.

[3] S. Bartariya and A. Rastogi, "Security in Wireless Sensor Networks: Attacks and Solutions," environment, vol. 5, 2016.

[4] F. Hu, W. Siddiqui, and K. Sankar, "Scalable Security in Wireless Sensor and Actuator Networks (WSANs)," Security in Sensor Networks, p. 177, 2016.

[5] S. S. Sran, L. Kaur, G. Kaur, and S. K. Sidhu, "Energy Aware Chain based data aggregation scheme for wireless sensor network," in 2015 International Conference on Energy Systems and Applications, 2015, pp. 113-117.

[6] Y. Yao, Q. Cao, and A. V. Vasilakos, "EDAL: An energy-efficient, delay-aware, and lifetime-balancing data collection protocol for heterogeneous wireless sensor networks," IEEE/ACM Transactions on Networking, vol. 23, pp. 810-823, 2015.

[7] I. Mahgoub and M. Ilyas, Sensor network protocols: CRC press, 2016.

[8] J. Yin and S. K. Madria, "A hierarchical secure routing protocol against black hole attacks in sensor networks," in IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), 2006, p. 8 pp.

[9] X. Du, M. Guizani, Y. Xiao, and H.-H. Chen, "Two tier secure routing protocol for heterogeneous sensor networks," IEEE transactions on Wireless Communications, vol. 6, pp. 3395-3401, 2007.

[10] F. Kausar, M. Q. Saeed, and A. Masood, "Key management and secure routing in heterogeneous sensor networks," in 2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2008, pp. 549-554.

[11] S. Madria and J. Yin, "SeRWA: A secure routing protocol against wormhole attacks in sensor networks," Ad Hoc Networks, vol. 7, pp. 1051-1063, 2009.

[12] S.-B. Lee and Y.-H. Choi, "A secure alternate path routing in sensor networks," Computer Communications, vol. 30, pp. 153-165, 2006.

[13] J. Yin and S. Madria, "SecRout: a secure routing protocol for sensor networks," in 20th International Conference on Advanced Information Networking and Applications-Volume 1 (AINA'06), 2006, p. 6 pp.

[14] K. Zhang, C. Wang, and C. Wang, "A secure routing protocol for cluster-based wireless sensor networks using group key management," in 2008 4th international conference on wireless communications, networking and mobile computing, 2008, pp. 1-5.

[15] L. Tang and Q. Li, "S-SPIN: a provably secure routing protocol for wireless sensor networks," in Communication Software and Networks, 2009. ICCSN'09. International Conference on, 2009, pp. 620-624.

[16] J. Zhou, C. Li, Q. Cao, and Y. Shen, "An intrusion-tolerant secure routing protocol with key exchange for wireless sensor network," in ICIA 2008. International Conference on Information and Automation, 2008., 2008, pp. 1547-1552.

[17] N. Gui, R. Chen, Z. Cai, J. Hu, and Z. Chen, "A secure routing and aggregation protocol with low energy cost for sensor networks," in IEEC'09. International Symposium on Information Engineering and Electronic Commerce, 2009. , 2009, pp. 79-84.

[18] F.-h. Cheng, J. Zhang, and Z. Ma, "Curve-based secure routing algorithm for sensor network," in 2006 International Conference on Intelligent Information Hiding and Multimedia, 2006.

[19] Y.-x. Jiang and B.-h. Zhao, "A secure routing protocol with malicious nodes detecting and diagnosing mechanism for wireless sensor networks," in The 2nd IEEE Asia-Pacific Service Computing Conference (APSCC 2007), 2007.

[20] S. Wen, R. Du, and H. Zhang, "A Segment Transmission Secure Routing Protocol for Wireless Sensor Networks," in 2006 International Conference on Computational Intelligence and Security, 2006.

[21] X. Yao and X. Zheng, "A secure routing scheme based on multi-objective optimization in wireless sensor networks," in CIS'08. International Conference on Computational Intelligence and Security, 2008. , 2008, pp. 436-441.

[22] C. Yin, S. Huang, P. Su, and C. Gao, "Secure routing for large-scale wireless sensor networks," in ICCT 2003. International Conference on Communication Technology Proceedings, 2003. , 2003, pp. 1282-1286.

[23] R. Vidhyapriya and P. Vanathi, "Energy aware routing for wireless sensor networks," in 2007 International Conference on Signal Processing, Communications and Networking, 2007, pp. 545-550.

[24] R. K. Gill, P. Chawla, and M. Sachdeva, "Study of LEACH Routing Protocol for Wireless Sensor Networks‖," in International Conference on Communication, Computing & Systems (ICCCS–2014).

[25] S. Roychowdhury and C. Patra, "Geographic adaptive fidelity and geographic energy aware routing in ad hoc routing," in International Conference, 2010, pp. 309-313.

[26] H. Kour and A. K. Sharma, "Hybrid energy efficient distributed protocol for heterogeneous wireless sensor network," International Journal of Computer Applications, vol. 4, pp. 1-5, 2010.

[27] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems," in Aerospace conference proceedings, 2002. IEEE, 2002, pp. 3-1125-3-1130 vol. 3.

[28] Q. Li, J. Aslam, and D. Rus, "Hierarchical power-aware routing in sensor networks," in Proceedings of the DIMACS workshop on pervasive networking, 2001.

[29] N. Sadagopan, B. Krishnamachari, and A. Helmy, "Active query forwarding in sensor networks," Ad Hoc Networks, vol. 3, pp. 91-113, 2005.

[30] A. Manjeshwar and D. P. Agrawal, "TEEN: ARouting Protocol for Enhanced Efficiency in Wireless Sensor Networks," in IPDPS, 2001, p. 189.

[31] A. Manjeshwar and D. P. Agrawal, "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks," in Ipdps, 2002, p. 48.

[32] T. He, J. A. Stankovic, C. Lu, and T. Abdelzaher, "SPEED: A stateless protocol for real-time communication in sensor networks," in Proceedings. 23rd International Conference on Distributed Computing Systems, 2003. , 2003, pp. 46-55.

[33] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in Proceedings of the 6th annual international conference on Mobile computing and networking, 2000, pp. 56-67.

[34] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer networks, vol. 38, pp. 393-422, 2002.

[35] J. Kleenankandy, "Mobile Networking For Smart Dust," Cochin University of Science and Technology, 2005.