Chapter

Wireless Sensor Networks (WSNs): Security and Privacy Issues and Solutions

Oladayo Olufemi Olakanmi and Adedamola Dada

Abstract

Wireless sensor networks (WSNs) have become one of the current research areas, and it proves to be a very supportive technology for various applications such as environmental-, military-, health-, home-, and office-based applications. WSN can either be mobile wireless sensor network (MWSN) or static wireless sensor network (SWSN). MWSN is a specialized wireless network consisting of considerable number of mobile sensors, however the instability of its topology introduces several performance issues during data routing. SWSNs consisting of static nodes with static topology also share some of the security challenges of MWSNs due to some constraints associated with the sensor nodes. Security, privacy, computation and energy constraints, and reliability issues are the major challenges facing WSNs, especially during routing. To solve these challenges, WSN routing protocols must ensure confidentiality, integrity, privacy preservation, and reliability in the network. Thus, efficient and energy-aware countermeasures have to be designed to prevent intrusion in the network. In this chapter, we describe different forms of WSNs, challenges, solutions, and a point-to-point multi-hop-based secure solution for effective routing in WSNs.

Keywords: wireless sensor network, encryption, routing protocol, security, privacy

1. Introduction

Wireless sensor network (WSN), as shown in **Figure 1**, is a wireless interconnected network which consists of independently setup devices that monitor the conditions of its environment using sensors. WSNs are employed in a wide range of applications such as security surveillance, environmental monitoring, target tracking, military defense, intrusion detection, etc. Security in wireless sensor network is at a growing stage mainly not because of nonavailability of efficient security schemes, but most of the existing schemes are not suitable due to the peculiarity of WSNs. That is, WSNs' nodes have low computational capacity and energy constraint. In WSNs, sensor nodes have the ability to communicate with one another, but their primary task is to sense, gather, and compute data. These data are forwarded, via multiple hops, to a sink which may use it or relay it to other networks. To achieve an effective communication, WSNs need efficient routing protocols [2–6]. They facilitate communication in WSNs by discovering the appropriate routes for transmitting data and maintain the routes for subsequent

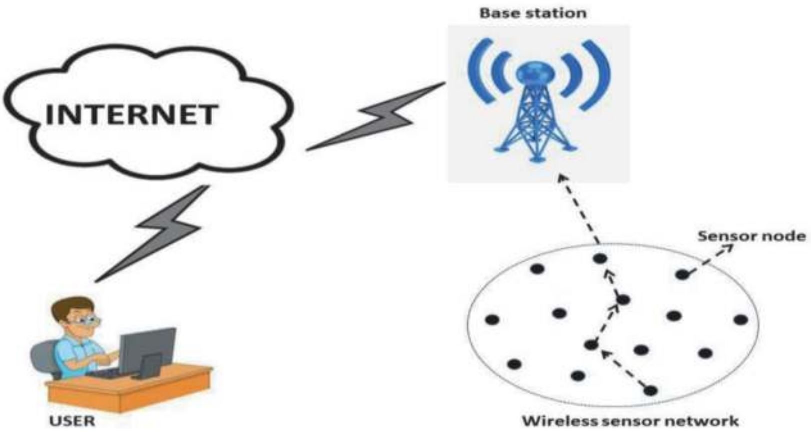

Figure 1.
A typical wireless sensor networks (WSN) [1].

transmissions. As a result of heterogeneity of WSNs' nodes, different protocols had been developed for different WSNs depending on the nature of the nodes and application. For instance, there are dedicated protocols for MWSNs and dedicated protocols for SWSNs.

There are two modes of transmission in WSN; single hop involves the source node sending its data packets to the destination within a hop. Meanwhile, WSNs' sensor nodes may rely on one another in order to relay packets to remote destinations. This mode of transmission is called multi-hop. Multi-hop is a routing phenomenon that involves the transfer of data between source and destination nodes with the cooperation of intermediary nodes. It enhances the performance of WSNs by allowing energy-depleted node to transfer data through its neighboring nodes along the routing path to the destination node. There are several security and privacy issues associated with multi-hop routing. Some of these issues like snooping, sinkhole, tampering Sybil, clone, wormhole, spoofing, etc. affect the integrity, availability, and data confidentiality of the WSNs.

Several security solutions had been proposed for WSNs; however, resource constraint of sensors makes some of these security solutions unfit for WSNs. This, therefore, makes their adoption in WSNs impossible. This is as a result of instability of the topology of most WSNs. Some of the WSNs, unlike some other networks, consist of mobile nodes that intermittently change the topology of the networks, therefore making it impossible for such mobile network to use existing protocol developed for static nodes. Also, large volume of data is transferred on the WSNs; this increases the traffic on the wireless communication infrastructure of WSN. All these show that security and privacy solutions of WSN must not only be lightweight in terms of the computational, communication, and energy overheads but also support aggregation and multi-hop in order to reduce the traffics and extend the life span of the networks. Meanwhile, most of the existing security solutions do not have these performance requirements [1, 7–10].

2. Classification of WSNs protocols

Routing protocols can be classified into:

1. Data-centric routing protocol

2. Hierarchical routing protocol

3. Multipath-based routing protocol

4. Location-based routing protocol

5. QoS-based routing protocol

6. Mobility-based routing protocol

2.1 Data-centric routing protocol

Data-centric routing protocol combines data arriving from various sensor nodes at a specific route. This eliminates redundancies and minimizes the total amount of data transmission before forwarding it to the base station. Directed diffusion, rumor routing, and sensor protocol for information via negotiation (SPIN) protocol are examples of data-centric routing protocol [11, 12].

SPIN is a negotiation-based data-centric protocol for WSNs. Each node uses metadata to name its data, and negotiation is performed by a sensor node using its metadata. Hence, each node is able to negotiate whether to deliver data or not, in order to eliminate redundant data transmission throughout the network. After the negotiation, the sender transmits its data as shown in **Figure 2**; node A starts by broadcasting its hop request to its neighboring node B. Once the request is accepted, node A sends its data to B who then repeats this procedure. This is to find its neighboring node and hops the data to the neighboring node until the data reaches the destination. SPIN protocol saves energy due to the fact that each node only performs single hop. SPIN's hop request and acceptance packets prevent flooding attack on WSNs. Although SPIN protocol is good for lossless networks, it can also be used for lossy or mobile networks.

2.2 Hierarchical routing protocol

Hierarchical routing protocol classifies network nodes into hierarchical clusters. For each of the clusters, the protocol selects a node with high residual energy as the cluster head. The sensed data of each node in the cluster are transferred through the cluster heads of the clusters in the network [11]. The cluster node aggregates the sensed data of all the nodes in the cluster before sending it to the sink. Hierarchical routing protocol reduces the energy consumption through multi-hop transmission mode [13]. Also, data aggregation performed by the cluster head reduces traffic on

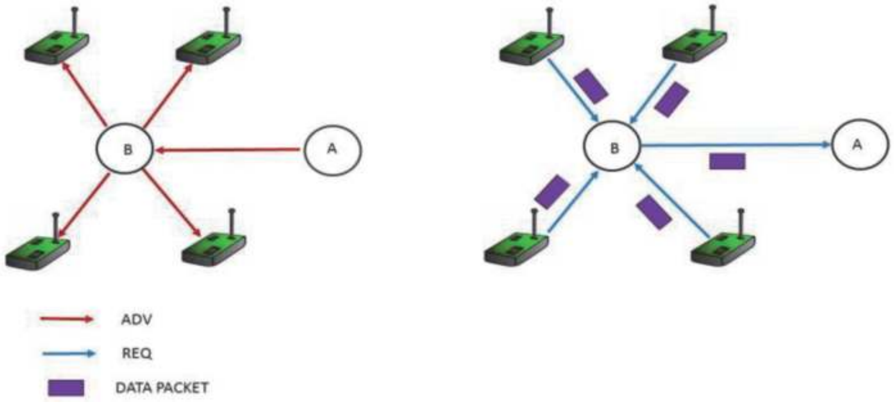

Figure 2.
SPIN protocol.

the network. Low-energy adaptive clustering hierarchy (LEACH), threshold-sensitive energy-efficient sensor network protocol (TEEN) and adaptive threshold-sensitive energy-efficient sensor network protocol (APTEEN), and secure hierarchical energy-efficient routing (SHEER) are examples of hierarchical routing protocol. TEEN gives a very good performance since it reduces the number of transmissions [14]. Patil et al. presented SHEER in [15]. It uses adaptive probabilistic transmission mechanism for determining the optimal route in WSN. SHEER also adopts hierarchical key establishment scheme (HIKES) for key distribution, authentication, and confidentiality. SHEER involves four phases as described below:

2.2.1 Initiation phase

1. The base station (BS), computes key $K_R = HMAC(I_R \| O_R)$, generates a broadcast authentication token N_R, and encrypts it as $N_R^l = Enc_{K_R}\ (N_R)$. The base station pre-loads each sensor node with N_R^l and keeps I_R and O_R.

2. BS broadcasts the initiation call as $N_b \parallel I_R \parallel O_R \parallel Enc_{K_R}\ \left(init \parallel N_b \parallel N_R \parallel N''_R\right)$, where *init* is the initiation call, O_R is the index, O_R is the offset of K_R, and N_b is time stamp generated by BS.

3. On receiving the initiation message, the sensor node extracts and decrypts $Enc_{K_R}\ \left(init \parallel N_b \parallel N_R \parallel N''_R\right)$, regenerates N'_R, and compares it with the N_R in the received initiation message. If they are similar, then the base station is successfully authenticated. It then replaces N_R in the newly with N'_R, sets its timer and starts the next phase.

2.2.2 Neighbor discovery phase

During the neighbor discovery phase, the sensor nodes establish their hopping link with their neighboring node. Each node switches from listening mode to transmission mode. In listening mode, node sends a HELLO message containing its identity, a nonce, and an encrypted header with the sensor key until it gets a reply from its neighboring nodes.

2.2.3 Clustering phase

In this phase, cluster consisting of certain number of nodes with a cluster head is selected based on some parameters.

2.2.4 Data message exchange phase

Each sensor sends its data to the base station through the cluster heads. This centralize data transmission reduces collision within clusters.

2.3 Multipath routing protocol

For an effective data delivery, multipath routing protocol generates a multipath (primary and secondary paths) from the source node to the destination node. It uses secondary path in case the primary path fails. With this, fault tolerance is achieved. However, this increases the cost of routing through the cost of maintaining multiple paths between source and destination [10, 16]. There are different types of multipath-based routing protocols.

2.3.1 Disjoint path routing protocol

In a disjoint path routing protocol, every source node finds the shortest disjointed multipath to the sink node. It evenly shares its data load among these disjointed paths. All the paths in this multipath share no sensor node. The protocol is reliable with extra overhead but at a low energy.

2.3.2 Braided path routing protocol

To construct braided multipath, the protocol first selects the primary path; then for every sensor, the best path is chosen from source to sink node, but this path does not include the primary node. The best alternative paths that are not necessarily disjoint from the primary path are called idealized braided multipath. These alternative paths are located either on the primary path or very close to it which means that the energy consumption on both the primary path and an alternative path is almost equal [17].

2.3.3 N to 1 multipath discovery routing protocol

N to 1 multipath discovery protocol is a protocol based on flooding. Example of N to 1 multipath-based routing protocol is multipath-based segment-by-segment routing (MSSR) protocol proposed by Lu et al. in [18]. MSSR protocol divides a single path into multiple segments, where multiple node-disjoint paths are discovered and independently maintained. N to 1 multipath discovery routing protocol reduces congestion, and effectively manages.

2.4 Location-based routing protocol

Location-based routing protocol routes data based on the distance of the source and destination nodes. It calculates the distance between source and destination nodes in order to determine estimated routing energy. Shruti [19] proposed a location-based routing protocol. The protocol uses the signal strength of the incoming signal to determine their distance. In their protocol, all the non-active nodes are put in sleeping mode in order to save energy. In location-based, the knowledge of the position of sensor nodes is exploited to route the query from the base station to the event. Location information enables the network to select the best route.

Another example of the location-based protocol is the geographic adaptive fidelity (GAF) protocol for mobile adhoc networks (MANETs). GAF conserves energy, and reduces routing overhead, which makes suitable for WSNs. Other examples of location-based protocols are location-aided routing (LAR), energy-efficient location-aided routing (EELAR), greedy location-aided routing protocol (GLAR), etc.

2.5 Quality of service (QoS)-based routing protocol

QoS-based routing protocol balances effective data delivery of the data to the sink node with some predetermined QoS metrics [17, 20]. Some of the existing QoS-based routing protocols are described below:

2.5.1 Sequential assignment outing (SAR) protocol

SAR protocol uses energy, QoS on each path, and the priority level of each packet as the QoS metrics to achieve effective data delivery. SAR protocol discovers and uses multiple paths from the sink node to sensor nodes for effective data delivery. SAR protocol considers energy efficiency and fault tolerance and also focuses on minimizing the average weighted QoS metric during data transfer [21].

2.5.2 SPEED protocol

SPEED is also an example of QoS-based routing protocol. In SPEED, every sensor node keeps its neighboring node information in order to increase the performance of the protocol. For example, SPEED protocol has congestion avoidance mechanism that is used to avoid congestion. The mechanism relies on the node information. Routing module in SPEED is called stateless geographic nondeterministic forwarding (SGNF) and works together with four modules at the network layer. In this protocol, the total energy used for transmission is incomparable to the performance of the routing algorithm.

2.5.3 QoS-aware and heterogeneously clustered routing (QHCR)

It is an energy-efficient routing protocol used by heterogeneous WSNs for delay-sensitive, bandwidth-hungry, time-critical, and QoS-aware applications. The QHCR protocol provides dedicated paths for real-time applications as well as delay-sensitive applications at a lower energy. The QHCR protocol consists of information gathering, cluster head selection, and intra-cluster communication phases.

2.6 Mobility-based routing protocol

Mobility-based routing protocol is a lightweight protocol that ensures data delivery from source to destination nodes. Tree-based efficient data dissemination protocol (TEDD), scalable energy-efficient asynchronous dissemination (SEAD), two-tier data dissemination (TTDD), and data MULES are some of the examples of mobility-based routing protocol. These routing protocols deal with the dynamism of the topology of the network. The closest node to the sink node tends to transmit more than others, which reduces its lifetime faster than other nodes [22]. Another example of the mobility-based routing protocol was the protocol proposed by Kim et al. [23]. The authors proposed a temperature-aware mobility algorithm for wireless sensor networks. Their algorithm employs store-and-carry mechanism to overcome the challenges posed by human postural mobility. In their store-and-carry-based routing protocol, routing packets are stored in a temporary memory called buffer. The buffer reroutes lost data to any intermediary node that temporarily lost connection with the source node. Their protocol also uses temperature to determine the intermediary node.

Another example of mobility protocol is the routing protocol proposed by Kumar et al. in [24]. They use ant colony optimization (ACO) and endocrine cooperative particle swarm optimization (ECPSO) algorithms to enhance the performance of the WSNs.

3. Security and privacy issues in WSN

Most of the existing WSN routing protocols and existing security solutions are unsuitable for WSNs. This is due to resources constraint associated with WSNs [25]. These constraints majorly determine the kind of security approaches that can be adopted for WSNs. Various security issues and their solutions are described in this section.

3.1 Security and privacy issues

The increase in demand for a real-time information has made WSN become more expedient. WSNs most of the time employs multi-hop transmission mode to overcome their constraints. The major problem of multi-hop transmission is attacks on the source data and nodes' identities during hopping. For a resource-constraint WSN with source node sending data to the destination through several intermediary nodes, there is a possibility of intrusion, identity tracing by an adversary, gleaning, and modification of source data by the intermediary nodes. WSNs, most times, operate in hostile environments and can be subjected to side channel attacks, such as differential power analysis. In these attacks, the adversary monitors the system, repeats the same operation, and takes careful measurements of power consumed in a cycle-by-cycle basis in order to either recover the secret key or perturb used in the perturbation. To prevent this, a scalar blinding is usually engaged in cryptographic-based security solutions. The scalar multiplication is blinded using integer m, where m is the order of the point $P \in E_q$, such that $mP = 0$. For example, instead of computing $Q = kP \; mod \; q$, $Q = (k + m)P \; mod \; q$ is computed.

Another issue in WSNs is how to preserve the identities of the source and destination nodes from the privy of intermediary nodes and adversaries during multi-hop. That is, there must be a form of lightweight authentication feature(s) inherent in the data packet between a source and destination nodes. Some other attacks on WSNs are discussed below.

3.1.1 Manipulating routing information

This attack targets the routing information between two sensor nodes. It can be launched through spoofing or replaying the routing information. This can be done by adversaries who have the capability of creating routing loops, attracting or repelling network traffic, and extending or shortening source routes. This attack is a passive attack which is not only easy to launch but elusive to detection. However, a unique identity can be created for the selected path (using key-based hash function of the pseudonyms or identity of all the selected intermediate nodes and embellishes in the message, any attempt to record data packet from a location and re-tunnel it at another location will be detected by the base station when comparing the embellished path identity with hash of all the appended pseudonyms or identities of all the nodes involved in the multi-hop).

3.1.2 Sybil attack

In this attack, adversary compromises the WSN by creating fake identities to disrupt the network protocols. Sybil attack can lead to denial of services. It may also affect mapping during routing, since a Sybil node creates illegal identities in a bid to break down the one-to-one mapping between each node. Sybil is common in P2P networks and also extends to wireless sensor networks [8]. Moreover, detection and defense against Sybil attack is more challenging; this is due to the limited energy and computational capabilities of WSNs. Different efforts had been developed to thwart Sybil attack in WSN. An example is the use of a pair-wise key-based detection scheme which sets a threshold for the number of the identity that a node can use [21]. However, this requires pre-assignment of keys to sensor node.

Another way to thwart Sybil attack is to validate identity of every node involved in routing. This can be reactively or proactively done. Reactively means prior to routing, a node must provide enough identification parameters to differentiate it from all other sensor nodes. The most common method is a resource test. Another way is to increase the cost against the benefit in identity generation [8]. That is, increasing cost of creating an identity and reducing the possible of having multiple identities will thwart Sybil attack, since the goal of a Sybil attacker is to acquire more identities. Also, traceable pseudonym and network-node identity generated by base station can be used to prevent a Sybil attack [9, 26].

3.1.3 Sinkhole attack

This attack prevents the sink node (base station) from obtaining the complete and correct data from the sensors, thus posing a threat to higher layer applications. In this attack, an adversary makes itself receptively attractive to its neighboring nodes in order to direct more traffics to itself [27, 28]. This results in adversary attracting all the traffics that is meant for the sink node. The adversary can then launch a more severe attack on the network, like selective forwarding, modifying, or dropping the packets. WSN is more vulnerable to this attack because its nodes most of the time send data to the base station [29].

Meanwhile, a point-to-point authentication between source node, identifiable intermediate nodes, and end-to-end symmetric encryption between source and destination nodes can be used prevent sinkhole, Sybil, and sinkhole attacks. The attack is foiled once the adversary could not decrypt end-to-end symmetric encrypted data even if it successfully impersonates the node and receives its data packet [9].

3.1.4 Clone attack

In a clone attack, the attacker first attacks and captures the legitimate sensor nodes from the WSNs, collects all their information from their memories, copies them on multiple sensor nodes to create clone nodes, and finally deploys them to the network. Once a node is clone, adversary can then launch any other attacks. There are two different ways of detecting this attack: centralized and distributed approaches. Centralized uses sink node to detect and foil the activities of clone nodes, while distributed approach uses selected nodes to detect clone nodes and foil their activities in the network. Distributed approach is suitable for static WSNs because distributed techniques use nodes’ location information to detect clones and sensor nodes with the same identity, but different addresses are taken as clone nodes. Meanwhile, in mobile WSNs, it is a different thing entirely, sensor nodes keep changing their position, and these nodes keep joining and leaving the network. Hence, node location information is not considered as the best technique for detecting clone nodes. Clone node can launch the following attacks:

3.1.4.1 Selective forwarding attack

Multi-hop-based WSN routing protocols assumed that all the neighboring nodes must re-hop their received data packets. Malicious nodes selectively forward some packets while dropping the others. Selective forwarding attacks are most effective when the adversary is actively involved in the data flow.

3.1.4.2 HELLO flood attack

This attack utilizes the connection between nodes. Most routing protocols require sensor nodes to broadcast HELLO packets to announce themselves to their neighboring nodes. An adversary may exploit this to deceive sensor nodes receiving the HELLO packet that they are within the radio range of the source node. In [30], the authors proposed a new method for detecting the HELLO flood attack based on distance. Here, nodes not only compare the RSS of the received HELLO packet but also compare the node's distance to the selected cluster head (CH) with the threshold distance. Only those nodes whose RSS as well as distance falls within the threshold limits are allowed to join the network. For example, in the setup phase of LEACH protocol [31], CH sends its own location coordinates. The nodes receiving HELLO packets from CH calculate the distance *Dist* as shown below:

$$Dist = sqrt[sq(x2 - x1) + sq(y2 - y1)]$$

Here, (x1; y1) are the coordinates of the sensor node receiving the packet, and (x2; y2) are the coordinates of CH. Each sensor node calculate the radio signal strength value (*RSS*) and distance between (*Dist*). These are used to determine the cluster they belong in, that is, if $(RSS < ThRSS \text{ } and \text{ } Dist < ThDist)$ then Node = 'Friend of the cluster' otherwise not a friend of the cluster.

3.1.4.3 Denial of service attack

This type of attack exploits the weaknesses in the sensor network, by attempting to disrupt the sensor network. Denial of service (DoS) attack denies services to valid users [32]. In a safety-critical network, this kind of attack can be disastrous to the functionality of the network. One of the methods engaged by adversary to launch DoS is by flooding the network with messages in order to increase traffics on the network. The DOS attack can be detected through proper filtration of incoming messages based on the contents and identifying nodes with high number of faulty messages. Faulty messages are detected by checking for the contradiction between messages sent by neighboring nodes [33].

3.2 Security and privacy solutions

Recently, application of WSN has gained massive attention leading to new security challenges and design issues [34]. In this section, we discussed relevant research efforts on the development of security schemes for WSN using different approaches such as effective key management, public key infrastructure (PKI), multiclass nodes, as well as grouping of nodes to improve the security of routing protocols in WSNs.

3.2.1 Use of effective key management

Du et al. presented a scheme with an example of an effective key management. Their scheme takes advantage of the high-end sensors in the heterogeneous networks. The performance evaluation and security analysis of their scheme show that the key management scheme provides better security with less complexity than the existing key management schemes [35]. The protocol pre-assigns a few keys in the L-sensor and a few keys to every H-sensor. This is because H-sensor is tamper-proof and has a larger memory than L-sensor. Their scheme uses asymmetric pre-distribution (AP) key management scheme since the number of pre-distributed keys in an H-sensor and in an L-sensor is different [12].

3.2.2 Use of effective public key infrastructure

Yu in [36] solved the security problem in WSN using the public key cryptography as a tool to ensure the authenticity of the sink node or base station. The approach consists of two phases; the first phase is node to sink handshake phase, where sink and sensor nodes set up session keys for secure data exchange. In the second phase, the session keys are used to encrypt data. Their scheme is very easy to implement, and requires a low computational power. The only limitation of their scheme is that all the participating nodes in the network have to agree on a common key prior to the exchange of data. However, any scheme based on a single key is vulnerable to the key compromise. That is, a compromised sensor node will not only compromise the shared key but also the whole network.

Also, Chen et al. [37] presented a PKI-based approach to ensure secure keys exchange in the WSNs. Their scheme provides key management mechanism for wireless sensor network applications that can handle sink mobility and deliver data to neighboring nodes and sinks without failure. They also presented a method for detecting and thwarting DoS attack and data authentication encryption.

3.2.3 Effective use of multiclass nodes

Du et al. [38] presents a new secure routing protocol for heterogeneous sensor networks (HSNs), which is a two-tier secure routing (TTSR) protocol. The TTSR protocol consists of both intra-cluster routing and inter-cluster routing schemes. The intra-cluster routing forms a minimum spanning tree (shortest path tree) among L-sensors in a cluster for data forwarding. In case of inter-cluster routing, data packets are sent by H-sensors in the relay cells along the direction from the source node to the sink node. The tree-based routing and relay via relay cells of TTSR make it resistant to spoofing, selective forwarding, and sinkhole and wormhole attacks.

Du [39] also proposed a novel QoS routing protocol that includes bandwidth calculation and slot reservation for mobile ad hoc networks (MANETS). Their QoS routing protocol takes advantage of the numerous transmission ability of multiclass nodes. Their protocol used three encryption keys:

1. A public key known by the sink and all other nodes

2. Node private key shared by two neighbor nodes and refreshed in the route discovery phase

3. A share primary key between node and sink node

The QoS routing protocol divides transmission data into different data slices. Each slice is route through a unique route of the discovered multipath.

3.2.4 Effective grouping of nodes to improve security of wireless sensor networks

In group-based WSN security scheme, the dominating node processes the sensed information locally and prepares the authenticated report for the destination node [40]. In this category, sensor nodes are grouped into smaller clusters wherein each cell assigns a special sensor node to carry out all the burden of relaying multi-hop packets. Hence division of labor is possible in the network, which makes the scheme to consume low power. Zhang et al. in [41] presented a group-based security

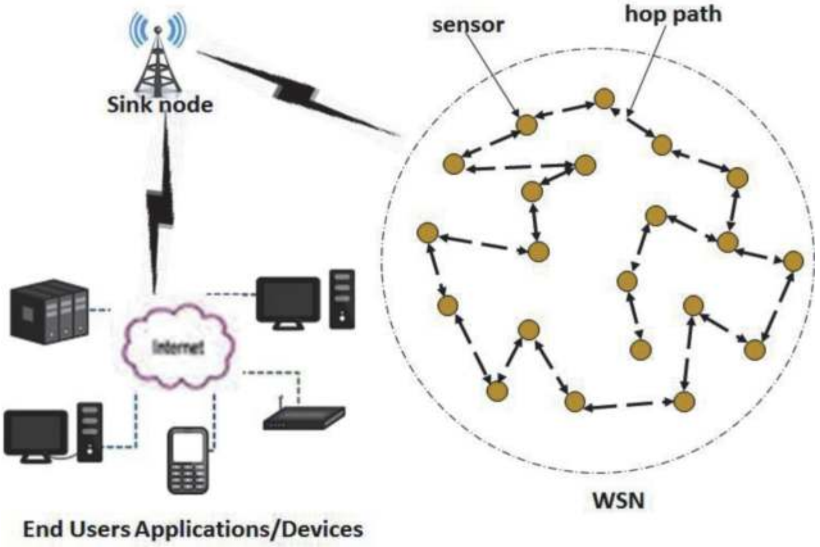

Figure 3.
Wireless sensor network system model.

scheme for distributed wireless sensor networks; their scheme involves three entities: one or more sink nodes, Y number of group dominator nodes, and N number of ordinary sensor nodes.

3.2.5 Point-to-point security solution

Point-to-point security solution involves secure routing between every two nodes along the multi-hop path. To show the design and efficacy of point-to-point solution, we fully describe a typical point to point security solution for multi-hop based WSNs proposed in [9]. Olakanmi and Dada [9] proposed an effective point-to-point security scheme that engages point-to-point (PoP) mutual authentication scheme, perturbation, and pseudonym to overcome security and privacy issues in WSNs. To reduce computational cost and energy consumption, they used elliptic curve cryptography, hash function, and exclusive OR operations to evolve an efficient security solution for a decentralized WSNs. The network model, as shown in **Figure 3**, consists of base station (BS), immediate node (IN), source node (SN) or (sn), and destination node (DS) or (ds). The SNs and DSs are capable of multi-hop transmission; therefore any SN can become DS and vice versa.

The PoP security scheme consists of the following phases: registration and key management, secure data exchange, perturbs generation, signature and obfuscation, authentication, and verification and decryption phases.

3.2.5.1 Registration and key management phase

The serial number ψ of each node is sent to BS. BS then generates unique pseudonym and network-node identity as follows:

i. BS randomly generates $s, \rho \in Z_q^* *$, as its master secret key pair, and computes and distributes its public parameter $\varphi = (\rho + \mu)P \ mod \ q$, where P is the generator of elliptic curve E_q and q is the order of E.

ii. Each node i randomly selects a unique $r_i \in Z_q^*$, computes its two-way distribution parameter β_i as β_i = $(r_i + \mu)P \ mod \ q$, and broadcasts its β_i to other nodes in the network.

iii. BS then computes N_i as $N_i = H(\rho \oplus \psi_i)$ and pseudonym F_i for each registered node as $F_i = H(N_i\|s\|\psi_i)$. It extracts the distribution parameter β_i of the node i in order to compute its node-base station shared key $\gamma_{bs\to i}$ as $\gamma_{bs\to i}$ = $\rho \ \beta_i$ and sends the symmetrically encrypted node's F_i and N_i as $E_{\gamma_{bs\to i}}$ (F_i) to node i.

iv. On the receipt of its encrypted pseudonym, each node then generates its corresponding node-base station shared key as $\gamma_{i\,\to\,bs}$ = $r_i\varphi$ and uses it to decrypt the received encrypted pseudonym.

3.2.5.2 Secure data exchange phase

To send data M, the primary SN signs M and generates perturb to secure M. It then encrypts the obfuscated message packet as σ, using its node-destination shared key $\phi sn\to ds$. The message packet σ contains the signature δ, perturbed data P_p, pseudonyms of the primary source node F_{sn}, and destination node F_{ds}.

3.2.5.3 Perturb generation phase

The perturbation enforces first level of security on the data. It is used to remove semantic pattern caused by wide variation in the transmitted data. The perturbation uses a novel additive noise generation method to perturb the data M. Primary source and destination nodes independently generate a set of perturb λ for session τ as follows:

i. The SN and its destination node generate their perturbation parameters α_{sn}, α_{ds} by randomly selecting a unique $m_1 \in Z_q^*$ and $m_2 \in Z_q^*$, and compute $\alpha_{sn} = (m_1 + \mu)P \ mod \ q$ and $\alpha_{ds} = (m_2 + \mu)Pmod \ q$, respectively.

ii. Using the destination perturbation parameter α_{ds} for session, SN computes perturbation seed ϑ as $\vartheta = m_1\alpha_{ds}$.

iii. For session, SN generates the perturbation chain as $\lambda = \{\lambda_1, \lambda_2, \lambda_3 \ldots \lambda_k\}$, where λ_1 = $H_\vartheta(\vartheta\| \ F_{sn})$, λ_n = $H_\vartheta(\lambda_{(n\ -\ 1)})$ for $n = 2 \ldots k$. Clear all the perturbation parameters of perturb index $n - 1$ in its memory for session τ and destination node of pseudonym F_{ds}. It replaces its former encrypted perturbation parameters with the new one, that is, replaces $[(\lambda_{n\ -\ 1}\|m_1\|$ $n - 1\|F_{ds}) \oplus \vartheta]$ with $[(\lambda_n\|m_1\|n\|F_{ds})\oplus \vartheta]$.

iv. Primary SN computes new perturb for every new data transmission of the same session by repeating step c using the previously used perturb λ_{n-1}. However, for a new session and destination node, SN generates a new ϑ by following steps (i)-(iii).

3.2.5.4 Signature and perturbation phase

Primary source node signs and perturbs the data packet through the following process:

a. Both the SN and destination nodes compute the source-destination shared session key $\phi_{sn \to ds}$ as follows:

   i. SN and destination nodes uniquely generate κ_1 and κ_2, respectively.

   ii. SN extracts the two-way distribution parameter of destination node β_{ds} to compute $\phi_{sn \to ds}$ as $\phi_{sn \to ds} = \kappa_1\beta_{ds}$.

b. Sign its data M using its source-destination shared session key $\phi_{sn \to ds}$ as $\delta = H\ \phi_{sn \to ds}\ (M)$, perturbs M as $P_p = M + \lambda_n$.

c. SN finally generates its message packet as $\sigma = \delta||P_p||F_i||F_j||n$, and encrypts it as $\sigma_\sigma = \sigma \oplus \phi_{sn \to ds}$ to further ensure second-tier data confidentiality and integrity of the message and communication information, where F_i and F_j are the pseudonyms of the source and destination nodes, respectively.

d. SN then performs PoP authentication with its IN, as described in the next section, before hopping P_p to the IN.

3.2.5.5 Authentication phase

After the signature and perturbation phase, the source node initiates the PoP authentication with the IN as follows:

i. SN generates an authentication token ω and time stamp t_s.

ii. SN and IN randomly generate $\upsilon \in Z_q^*$ and $\varepsilon \in Z_q^*$, respectively. SN computes its PoP authentication parameter as $n_{sn} = (\upsilon + \mu)P\ mod\ q$, while IN computes its own as $n_{in} = (\varepsilon + \mu)P\ mod\ q$ and sends it to SN, who then computes its PoP session authentication key $\varphi_{sn \to in}$ as $\varphi_{sn \to in} = \upsilon.n_{in}$.

iii. SN then encrypts the concatenated authentication token ω, pseudonym of source, pseudonym of IN, and time stamp as $E\varphi_{sn \to in}\ (\omega||F_{sn}||F_{in}||t_s)$, concatenates it with n_{sn} as $E\varphi_{sn \to in}(\omega||F_{sn}||F_{in}||t_s))||n_{sn}$, and sends it to its IN.

iv. On the receipt of $E\varphi_{sn \to in}(\omega\ ||F_{sn}||F_{in}||t_s)||n_{sn}$, IN extracts n_{sn} then computes its $\varphi_{in \to sn} = \varepsilon.n_{sn}$. It decrypts the received $E\varphi_{sn \to in}(\omega||F_{sn}||F_{in}||t_s)$ using its $\varphi_{sn \to in}$ to extract ω and t_s. It, thereafter, re-encrypts the extracted ω and t_s, using $\varphi_{in \to sn}$, and sends it back to the SN. The SN decrypts it using its $\varphi_{sn \to in}$ and verifies it by comparing the ω and t_s with their original values. If equal, SN hops its encrypted data packet σ_σ. The IN then becomes temporary SN and repeats this phase with its selected IN until the packet gets to the destination node.t

3.2.5.6 Verification and decryption

Destination node extracts and authenticates the received data M by following this procedure:

i. Destination node extracts the two-way distribution parameter of SN and βsn and computes destination of the used perturb P.

ii. Destination node regenerates the used perturb λ'_n by checking the value on the perturb index n. If $n = 1$, it indicates that the source is new to the destination node, and destination node then executes perturbation generation phase in order to obtain the perturb seed, which would be used to recompute the used perturb. However, if $n > 1$, it indicates that the session is for old destination node. The destination node retrieves the encrypted last perturb for the source node from its memory, decrypts it, and uses it to obtain the used perturb by executing step 3 of the perturbation generation phase. Extract the n message by unperturb P_P as: $M' = P_P - \lambda'_n$.

iii. Destination node verifies the signature by re-signing the unblinded message M' using its $\phi_{ds \to sn}$ as $\delta' = H\phi_{ds \to sn} (M')$. If $\delta' = \delta$, then the perturb, data, and the source node are all valid, and destination node then accepts the data, otherwise rejects the data. Encrypt the perturbation parameter as $\lambda_n \oplus \vartheta$, $m_2 \oplus \vartheta$, $n \oplus \vartheta$, F_{sn}. Clear all the previously encrypted perturbation parameters stored for F_{sn} in its memory, and replace it $(\lambda n||\vartheta||m2||\vartheta||n)$.

4. Conclusion

This chapter shows overview of wireless sensor networks with its security and privacy framework. The chapter proffers to readers an in-depth understanding of security and privacy issues as related to WSNs. Some existing research in WSN routing protocols are discussed. This chapter also helps researchers to understand the current trends in WSNs routing protocols and security schemes.

Author details

Oladayo Olufemi Olakanmi* and Adedamola Dada
Department of Electrical and Electronic Engineering, University of Ibadan, Nigeria

*Address all correspondence to: olakanmi@mit.edu

References

[1] Oladayo O, Abass A. A secure and energy-aware routing protocol for optimal routing in mobile wireless sensor networks (MWSNs). International Journal of Sensors, Wireless Communications and Control. 2019;**9**(Pt 4)

[2] Sohrabi K, Gao J, Ailawadhi V, Pottie GJ. Protocols for self-organization of a wireless sensor network. IEEE Personal Communications. 2000;**7** (Pt 5):16-27

[3] Villalba LJG, Orozco ALS, Cabrera AT, Abbas CJB. Routing protocols in wireless sensor networks. International Journal of Medical Sciences. 2009:8399-8421

[4] Messaoudi A, Elkamel R, Helali A, Bouallegue R. Cross-layer based routing protocol for wireless sensor networks using a fuzzy logic module. In: Paper Presented at the 13th International Wireless Communications and Mobile Computing Conference (IWCMC); 2017

[5] Huei-Wen DR. A secure routing protocol for wireless sensor networks with consideration of energy efficiency. In: IEEE National Taiwan University of Science and Technology; 2012. pp. 224-32

[6] Murugaboopathi G, Khaana V. Reliable communications in sensor networks. Journal of Engineering and Applied Science. 2008;**3**:911-917. Available from: https://medwelljournals.com/abstract/?doi=jeasci.2008.911.917 [Accessed: 10 July 2017]

[7] Saraswati M, Prabhjot K. Energy efficient neighbor selection for flat wireless sensor networks. Information Technology and Management. 2013: 518-523

[8] Lv S, Wang X, Zhao X, Zhou X. Detecting the Sybil attack cooperatively in wireless sensor networks. In: Paper Presented at the International Conference on Computational Intelligence and Security; 2008

[9] Olakanmi O, Dada A. An efficient point-to-point security solution for multi-hop routing in wireless sensor networks. Security and Privacy. 2018

[10] Oladayo O, Adama P. An efficient multipath routing protocol for decentralized wireless sensor networks for mission and safety-critical systems. International Journal of Sensors, Wireless Communications and Control. 2019;**9**(Pt 4)

[11] Jamil I, Imad M. A secure hierarchical routing protocol for wireless sensor networks. In: Paper Presented on the 10th IEEE International Conference on Communication Systems; Singapore; 2006

[12] Du X, Xiao Y, Chen H-H, Wu Q. Secure cell relay routing protocol for sensor networks. Special Issue on Network Security. 2009;**6**(Pt 3): 375-391

[13] Masruroh SU, Sabran KU. Emergency-aware and QoS based routing protocol in wireless sensor network. In: Paper Presented at the IEEE International Conference on Intelligent Autonomous Agents, Network and Systems; 2014

[14] Manjeshwar A, Agrawal DP. TEEN: A routing protocol for enhanced efficiency in wireless sensor networks. In: Proceedings of 15th International Parallel and Distributed Processing Symposium; IPDPS; 2009-2015; San Francisco; 2001

[15] Patil M, Biradar RC. A survey on routing protocols in wireless sensor networks. In: Paper Presented at the

18th IEEE International Conference on Networks; Mandya; 2012

[16] Durrani N, Kafi N, Shamsi J, Haider W, Abbsi A. Secure multi-hop routing protocols in wireless sensor networks: Requirements, challenges, and solutions. In: Paper Presented at the 8th IEEE International Conference on Digital Information Management (ICDIM); 2013

[17] Goyal D, Tripathy MR. Routing protocol in wireless sensor networks: A survey. In: Paper Presented at the IEEE International Conference on Advanced Computing and Communication Technologies; Haryana; January 2012

[18] Lu Y, Wang G, Jia W, Peng S. Multipath-based segment-by-segment routing protocol in MANETs. In: Paper Presented at the 9th International Conference for Young Computer Scientists; Hunan; November 2008

[19] Shruti UK. Few locations based routing protocols in wireless sensor network. In: Paper Presented at International Conference on Green Computing and Internet of Things (ICGCloT); Chennai; 2015

[20] Amjad M, Afzal MK, Umer T, Kim B-S. QoS-aware and heterogeneously clustered routing protocol for wireless sensor networks. IEEE Access. 2017;**5**:10250-10262

[21] Raghunandan GH, Lakshmi BN. A comparative analysis of routing techniques for wireless sensor networks. In: Paper Presented at the IEEE Conference on Innovations in Emerging Technology; 2011. pp. 17-22

[22] Krishna KK, Augustine R. A survey on mobility based routing protocols in wireless sensor networks. International Journal of Computer Applications. 2016; **135**(5):36-38

[23] Kim B-S, Kang SY, Lim JH, Kim KH, Krishna KK, Augustine R. A survey on mobility based routing protocols in wireless sensor networks. International Journal of Computers. 2017

[24] Kumar J, Tripathi S, Tiwari RK. Routing protocol for wireless sensor networks using swarm intelligence-ACO with ECPSOA. In: Paper Presented at the International Conference of Information Technology; 2016

[25] Obaidat MS, Li J-S. Security in wireless sensor networks. Security and Communication Networks. 2016;**1** (Pt 1):101-103

[26] Zhang J, Varadharajan V. A new security scheme for wireless sensor networks. In: IEEE Global Communications Conference (GLOBECOM) Proceedings; Hong Kong; 2008. pp. 1-5

[27] Qi J, Hong T, Xiaohui K, Qiang L. Detection and defence of sinkhole attack in wireless sensor network. In: Paper Presented at the IEEE 14th International Conference on Communication Technology; Chengdu; 2012

[28] Amisha P, Vaghelab VB. Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol. In: Paper Presented at the 7th International Conference on Communication, Computing and Virtualization; 2016

[29] Ahmad Salehi S, Razzaque MA, Naraei P, Farrokhtala A. Detection of sinkhole attack in wireless sensor networks. In: Paper Presented at the IEEE International Conference on Space Science and Communication (IconSpace); 2013

[30] Magotra S, Kumar K. Detection of HELLO flood attack on LEACH protocol. In: Paper Presented at the IEEE

International Advance Computing Conference (IACC); 2015

[31] Xiangning F, Yulin S. Improvement on LEACH protocol of wireless sensor network. In: Paper Presented at the IEEE International Conference on Sensor Technologies and Applications; 2007

[32] Raymond DR, Midkiff SF. Denial-of-service in wireless sensor networks: Attacks and defences. IEEE Pervasive Computing. 2008;**7**(Pt 1):74-81

[33] Ramkumar M. Proxy aided key pre-distribution schemes for sensor networks. In: Paper Presented at the IEEE International Conference on Performance, Computing, and Communications; 2010. pp. 461-68

[34] Gungor VC, Lu B, Hancke GP. Opportunities and challenges of wireless sensor networks in smart grid. IEEE Transactions on Industrial Electronics. 2010;**57**:3557-3564

[35] Du X, Guizani M, Xiao Y, Chen H-H. An effective key management scheme for heterogeneous sensor networks Francisco; December 2006

[36] Yu Z. The scheme of public key infrastructure for improving wireless sensor networks security. In: Paper Presented at the IEEE International Conference on Computer Science and Automation Engineering IEEE Transactions; Manchester; 2012

[37] Chen J-L, Lai Y-F, Lu H-F, Kuo Q-C. Public-key based security scheme for wireless sensor network. In: IEEE Radio and Wireless Symposium 2008. pp. 255-258

[38] Du X. Two tier secure routing protocol for heterogeneous sensor networks. IEEE Transactions on Wireless Communications. 2007; **6**(Pt 9):3395-3401

[39] Du X. QoS routing based on multi-class nodes for mobile. Ad Hoc Networks. 2004;**2**(Pt 3):241-254

[40] Abdul Hamid M, Mustazur Rahman M, Yoon YJ, Hong CS. Developing a group-based security scheme for wireless sensor networks. In: IEEE Global Communications Conference (GLOBECOM) Proceedings; 2007

[41] Li-Ping Z, Yi W, Gui-Ling L. A novel group key agreement protocol for wireless sensor networks. In: Paper Presented at the International Conference on Wireless Communication and Signal Processing; Beijing; 2009