https://doi.org/10.26438/ijsrcse/v6i3.5666

International Journal of Scientific Research in Computer Science and Engineering
Vol.6, Issue.3, pp.56-66 , June (2018)

Survey Paper

E-ISSN: 2320-7639

A Survey of Civilian Applications of WSN and Security Protocols

Chahat Aggarwal[1*], B. B. Gupta[2]

[1]Dept. of Computer Engineering, National Institute of Technology, Kurukshetra, India
[2]Dept. of Computer Engineering, National Institute of Technology, Kurukshetra, India

Available online at: www.isroset.org

Received: 24/May/2018, Revised: 03/Jun/2018, Accepted: 20/Jun/2018, Online: 30/Jun/ 2018

***Abstract*-** Wireless sensor networks have become an integral part of the modern smart living. There are a variety of applications of WSNs be it military, industry or civilian. With a multitude of gen – next applications of WSNs comes the responsibility of securing them. Owing to this fact many security protocols have been put forward in the past. In this paper, we discuss various civilian applications of WSNs and also review evolution of key distribution schemes.

***Keywords*-** Civilian applications, WSN security mechanisms

I. INTRODUCTION

The very first applications of WSN were in the field of the military such as in communication infrastructure, battlefield surveillance and enemy tracking. Since then till now, the applications of wireless sensors have grown by leaps and bounds.

The widespread development in Micro Electro Mechanical Systems (MEMS), distributed computing and wireless communications have led to extensive research and development in civilian applications of Wireless Sensor Networks. Undoubtedly, WSNs have become an inevitable part of environment monitoring systems be it agriculture, forestry, livestock or ecosystem monitoring, smart cities, smart traffic, and e-health. In this paper, we review the state of the art civilian applications of WSNs. We also discuss the system requirements for all the types of applications. These researches have shown that wireless sensor networks provide a better, convenient and alternate way of living [1]. Deploying sensors for the tasks earlier done by man also improves the system performance by fulfilling the functional requirements.

A wireless sensor network is a sequential combination of 4 units: a sensing unit, a processing unit, a communication unit, and a power unit. The sensing unit comprises of a group of transceivers that sense the environment for the desired stimulus and an ADC that converts analog signals to digital signals. These signals are then passed on to the processing unit that processes these signals with the help of a microprocessor. These processed signals are then passed on to the communication unit. Here the transceiver communicates the sensed stimulus to the end user. Finally, it is the power unit that powers all the operations of the sensor motes.

Secure communication in WSN calls for clever solutions. The main restraints that hamper the various security protocols are low battery life of the sensor nodes and the need to conserve the bandwidth. Also, the sensor motes are many a times easily physically accessible, thereby making them vulnerable to captured physically. Thus, efficient light weight solutions are required for securing these wireless sensor networks.

The paper is structured as follows: Section 2 describes various civilian applications of WSN. Section 3 gives an overview of attacks on WSN. Sections 4 and 5 explain in detail various key distribution schemes used in WSN and WBAN respectively. Section 6 finally concludes the paper.

II. APPLICATION OF WSNS IN VARIOUS DOMAINS

In this section, we explore various different civilian applications of Wireless Sensor Networks. These applications can be broadly classified under the domain of agriculture, smart parking, smart living spaces, and e-health. Each of the subsection describes different categories of applications under each domain.

2.1. Agriculture

Modern day agriculture and farming demand enhanced food production, intelligent information processing, greater productivity, fault tolerance and water conservation. WSNs cater to all these needs by providing novel and intelligent agricultural solutions.

In this section, we discuss the state of the art applications of WSNs in the agriculture domain.

Irrigation Management: Moghaddam et al [2] proposed the smart sensor web (SSW) in 2010. The spatial-temporal soil moisture variations in an intelligent control system guide the SSW in determining an optimal strategy for sensor configuration in the field. Along with the optimal strategy, the control system also provides estimation strategy after observing the soil moisture levels in all the dimensions. The task of suffering the configuration of the sensors is done by the actuators present at different depths. These actuators send the information to the central coordinator that then decides the time when future readings have to be taken.

In 2011 Saha et al [3] presented the Alfalfa crop irrigation system to stop the drainage of tail water in alfalfa crop. The authors devised a WSN based solution that completely eliminates water runoff by providing information about irrigation from the field and cellular communication along with a water advance model are used for wetting the field. Also, the farmers an SMS notification for shutting the water supply thereby reducing the water wastage.

Gutierrez et al [4] in 2014 put forward an automatic irrigation system to conserve water by reducing water usage. In order to measure soil moisture level at different depths soil moisture and temperature, sensor nodes are used: The automatic irrigation control system takes on the fly decision based on the values provided by the sensors. This irrigation control functions by itself whenever any of the two parameters exceed the threshold value. The remote server stores all the information and displays in a GUI fashion to the end user.

Aqua management Inc designed the AMI Turf Irrigation System to provide affordable water management solutions. This all in one irrigation system employees a cloud-based control system that measures various parameters like weather conditions, Evapotranspiration (ET), water leakage and flow. The application has a simple click-based user interaction with features such as remote programming, dynamic parameter adjustment water budgeting fault detection and alert notification. The AMI Q collects all the data from the sensors and consequently uploads the information on the cloud.

Diaz et al [5] put forward a vineyard production monitoring design using WSN to measure differences in agricultural parameters across the field. On basis of soil, geographic and weather maps the entire field is divided into different zones in the first phase. The second phase is the network planning phase. In this phase depending on the requirement of the application, an appropriate architecture is selected. In practice sensors are deployed in different areas of the field that collect the data about various parameters like temperature, luminosity, humidity etc. and route the information to the gateway. The irrigation system is driven by the actuators. The information routing is aided by the redundant nodes. These nodes also imitate the faulty nodes in function. Gateway is the bridge between the sensor nodes and the base station.

Cambra et al [6] suggested a video sensing mechanism for administering fertilizer consumption in agriculture. The objective of the proposed work is to maintain energy efficiency even by reducing the fertilizer consumption for crops. This objective is realized by using AR drones that record a video of the agricultural land. On the basis of this video, the system recognizes and positions the already present weeds in the farm. Finally, the actuator signals the sprayer system to spray the fertilizers only on crops and avoiding the weeds.

The Common – Sense Net [7] is a joint venture of EPFL, Zurich, and center for Electronic Design and Technology (CEDT) at IISC. The project was designed to predict and solve problems of unfavorable climate changes. The design consists of nodes measuring soil moisture at a depth of 30 cm and 150 cm both, amount of water needed for irrigation, temperature and humidity 9 on the field and 3 backward nodes send the collected data to the base station that then further sends the received data to the remote server via GPRS links.

Other applications in this domain include Pest and disease control [8] [9], controlled fertilizer spray [10], cattle movement tracking [11], greenhouse monitoring [12], and remote diagnosis[13]

2.1.1. Developments in India

IIT Kharagpur developed low-cost irrigation management system specifically for India.

Das et al [14] studied the most common fungal diseases in grapes with the help of agro- metrological sensors at Sulla vineyards, Nashik. Using sensors helped them in predicting this weather-related disease and hence benefited the grapevine industry manifold by increasing revenue and enriching quality of food.

Similarly, Shah et al [15] developed the Agri Sense distributed system to predict the Bud Necrosis Virus (BVN) in groundnut plant. The experimental setup was done at the AGNR Agricultural University, Hyderabad.

2.2. Environment Monitoring System

Environment monitoring systems are designed to sense monitor and control environmental parameters like temperature, humidity, luminosity, wind pressure etc. Some research is targeted towards proceeding highly accurate

solutions while others focus on fault tolerance. Thus, it is extremely vital to fathom the requirements of environment monitoring systems [16]

2.2.1. System Requirements for Environment Monitoring Systems

Autonomy

Proper functioning of the battery is inevitable as the radial transceiver consumes a lot of energy and the network should be energy efficient.

Reliability

To avoid unexpected system crashes the operations are required to be predictable and handling simple. Also, frequent maintenance is not advised as the end user may not be proficient enough and also may not have enough networking knowledge. Thus, the reliability of the system is very important

Robustness

Robustness is required to handle problems such as poor signal connectivity and hardware crashes.

Flexibility

Depending on the situation and requirement the user must be able to change, move or add stations to already existing systems.

2.2.2. Smart home applications of WSN

The concept of smart home emerged in the 1980s with an intent to provide assisted living. The focus shifted to taking care of the elderly in the home only in the 1990s. Today smart homes provide customized help according to the requirements of the individual.

Hue et al [17] work integrate WSN with RFID to measure a person's drug intake. It then transfers the ECG data reliably in a smart home environment.

Wen et al [18] present yet another technique for movement tracking by integrating WSN with machine learning. Such devices provide assisted living to the elderly.

Lec et al [19] present a methodology for designing access points so as to ascertain network efficiency by employing genetic algorithms.

2.3. Smart Parking Application of WSN

Parking has become a common problem in almost all the major cities. It often leads to air pollution, road congestion, and driver frustration. To eliminate all such parking related problems in Europe, Japan and U.K. were the first countries that implemented smart parking solutions. Smart parking systems provide a number of advantages:

Space availability: These systems alert the driver about the vacant parking slots.

Smooth Transit: People at parks and other public places can smoothly plan their transit with the help of such systems.

Estimating pricing Strategy: The parking administers / operator can use smart parking technology to regulate the pricing strategy depending on traffic trends.

Prevent vehicle thefts: These systems keep a 24/7 check on vehicles and alert any theft.

Expense Reduction: Smart parking system also reduces staff requirement thereby reducing expenses on staffing.

The work of Chen et al [20] introduced parking guidance and information system by deploying a WSN. The proposed system uses tree-like topology to transmit data via the WSN. It uses a non-standard protocol for this purpose. The data is processed by the information and management center and then displayed on LED servers for drivers.

A Transit based smart parking system deployed in Europe [21] uses loop detectors for the surveillance of available parking slots. The corresponding information is then sent via VMS signal.

Mouskos et al [22] developed a smart payment system for parking charges using WSN and RFID tags. The user activates the RFID unit at the onset of his parking and deactivates at his transit. Bills are displayed on the transit but actual payment is done on monthly bases.

U.Manni [23] proposed an online parking reservation system to reduce the time spent in finding a vacant slot for parking. Such a system also eliminates the need to pay extra fees for parking. Smart sensing technology is used to achieve the above-mentioned goal.

The work by Serpen et al [24] presented algorithms for fully automated parking system. Robot carts are used to park the vehicles in the parking area and elevators are used to move across floors.

2.4. E-Health applications of WSN

Suryadip et al [25] put forward a non- invasive, continuous monitoring application of WBASN for people suffering from Parkinson's disease. The patient is required to wear a shoe that has WSN device attached to it. This device continuously monitors the gait of the patient to recognizes any occurrence of freezing of gait (FOG) using the RSSI value. This is helpful in detecting and also preventing injuries and falls.

The major advantage of this shoe includes: It is an indoor monitoring system and there is no requirement of placing a number of sensor motes in the entire house to record movements of the patient. The shoe does the job!

Yan et al [26] put forward a WSN application for e-health to monitor a person's movement. This data can be directly sent to the doctor, relatives, caretakers etc or stored for future analysis. Also, this application provides tracking and localization in multiple rooms.

Authors in [27] proposed a Bluetooth - enabled in-home patient monitoring for early detection of Alzheimer's disease. Local movement of the patient is monitored and recorded using short-range Bluetooth technology. This allows the doctor to perform remote diagnosis through the internet.

The work of Chen et al [28] proposes an e-health care management system using second generation RFID technology. Using this technique the systems are able to perform on – demand actions according to the need of different objects.

III. ATTACKS IN WSN

3.1 Terminology of the terms used

In this section we adapt definitions of various terms related to attacks in WSN from the National Information Systems Security Glossary [29].

Threat: Any circumstance or event (such as the existence of an attacker and vulnerabilities) with the potential to adversely impact a system through a security breach.

Attack: Attempt to gain unauthorized access to a service, resource, or information, or the attempt to compromise integrity, availability, or confidentiality. Note that success is not necessary.

Attacker, Intruder, Adversary: We use these terms synonymously to mean the originator of an attack.

Vulnerability, Flaw: Weakness in system security design, implementation, configuration or limitations that could be exploited.

Risk: Probability that an attacker will exploit a particular vulnerability, causing harm to a system asset.

3.2. Attack Models

WSN is especially vulnerable to external and internal attacks due to the following peculiar characteristics:

Computational capabilities: These sensor nodes are used and throw devices and are generally equipped with the very less computational facility to lower the cost of the overall setup.

Memory: only a small microprocessor chip is embedded in the sensors and no additional memory element is generally attached

Communication bandwidth: the channels used are public channels (433 MHz ISM band) therefore the communication over these channels can be easily intercepted by anyone.

Battery power: the biggest concern is the battery power. These nodes are not powered by any outside energy source so they get exhausted soon. Security algorithms which are power efficient need to be developed to fully avail the services provided by WSNs.

Easy to physically access such nodes: They are generally deployed in areas where the nodes can be physically accessed. The intruder thus gains the privilege of tampering the hardware to assess the node id and easily implement an impersonation attack [30].

It thus becomes crucial to study and understand the varied types of attacks in order to prevent them. This section describes the attack models for the random and regular topology.

- Wormhole Attack: The adversary establishes an out of band communication channel between two sensor nodes. This fools the sensor nodes to think that they are neighbors to each other. This completely changes the routing information and the packets are tunneled from one part of the network to another. Thus, the adversary gains tremendous power by mounting a wormhole attack by monitoring the network traffic or even by mounting a DOS attack. The biggest challenge in overcoming wormhole attack is that even encryption techniques lie helpless in preventing this attack (Figure 1).

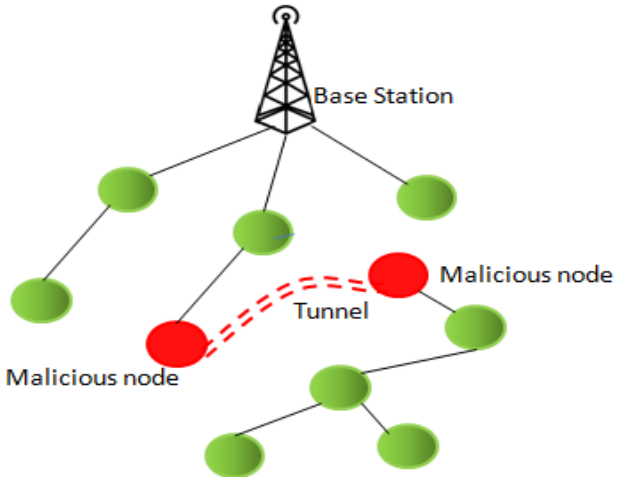


Figure 1: Wormhole attack

- Sybil: The corrupted node assumes a large number of identities at the time of routing. Thus, the malicious node is confused to be a legitimate node. Multipath routing gets severely affected by Sybil

attack, because the node may think that it is routing pockets via different paths, but in reality, all those paths may pass through the corrupted node. When combined with wormhole attack, it can have a devastating effect on the network.

- Spoofed or replayed routing information: This is the simplest type of attack that can be mounted on sensor nodes. The adversary aims at consuming critical network resources by injecting altered control pockets in the network (Figure 2). This leads to :
  - Attraction or repulsion of network traffic according to the attackers will.
  - Extension or shortening of routes
- Generation of the incorrect error message
- Sinkhole: The corrupted node lures roughly all traffic of the network by advertising false routing update. After receiving all the network information, the corrupted node gains the advantage of modifying the secret information about the network. Some routing protocols require the nodes to send hello packets to determine their neighbors
- Hello flood attack: The attacker that has high transmission power exploits this concept by sending or replaying these hello packets. The routing protocol gets disrupted as the attacker fools other nodes to believe that it is a neighbor to them. By broadcasting packets at much higher power, the corrupted node can even force legitimate nodes to elect its parent node (Figure 7).

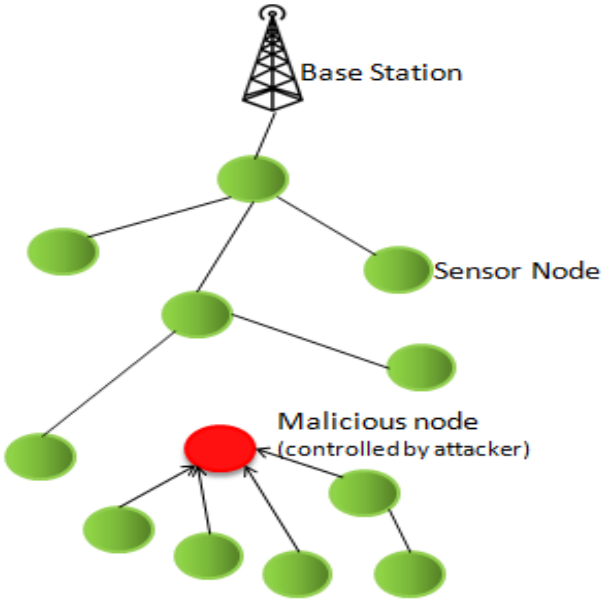


Figure 2: False routing information

- Acknowledgment Spoofing: In some routing protocols the SNs send back acknowledgments. The adversary may spoof these acknowledgment packets, thereby convincing other nodes that a weak link is a strong one or a dead SN is alive. Thus packets sent through these links may be lost or corrupted.

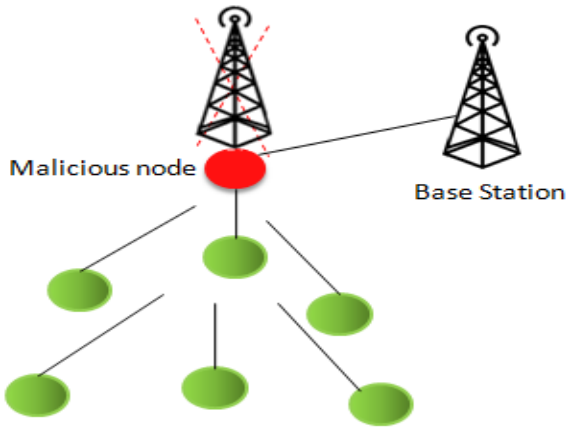


Figure 3: Hello Flood attack

IV. WSN SECURITY TECHNIQUES

All sensor nodes in WSN use power efficient radio transceivers for their communications. Regardless of the underlying technology of the transceiver, all communications are done through a wireless channel. As a result the information can be easily accessed by anyone in the vicinity. All packets are then unprotected against any kind of communication attack. It is indispensable to provide basic security primitives to the sensor nodes in order to give a minimal protection to the information and a foundation to create secure protocols. The security primitives are:

- Key Distribution and Management
- Symmetric Key Cryptography (SKC)
- Hash primitives
- Public Key Cryptography (PKC).

4.1. Key Management and Distribution

Key distribution and management is the heart of WSN security. In order to establish trust among nodes public and private keys are distributed among them. Since the nodes are highly resource constraint, therefore many lightweight schemes have also been proposed over the ages. When it comes to WSN three important tasks need to be performed with keys namely (Figure 4):

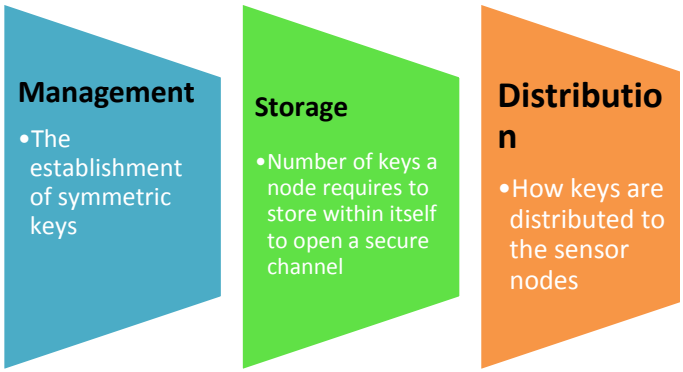


Figure 4: Management, storage, and distribution of keys

Numerous key distribution schemes have been suggested by researches in the past. A broad classification of these schemes is shown in figure 5.

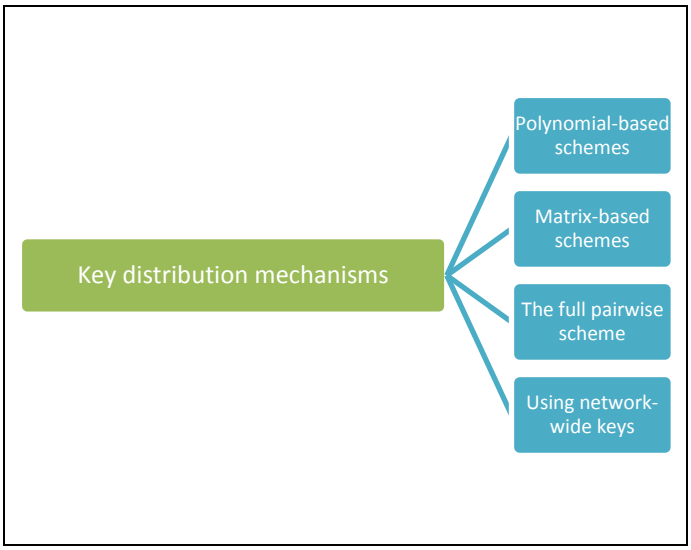


Figure 5: Taxonomy of key distribution mechanisms

4.1.1 Using Network Wide Keys

It is the simplest key distribution scheme. The single master key is loaded into all sensors that provide perfect key connectivity. An example of this approach is BROadcast Session Key Negotiation Protocol (BROSK)[30]. Any two nodes share random nonce, say N_a and N_b, along with the single master key to establishing a secure session key (Figure 10). However, the author makes the assumption that the shared master key is never divulged. This is key on which the node can tell whether another node is in the same network or not. Also, it is assumed that the master key cannot be extracted from the captured node.

The scheme works in the following manner:

Each node tries to broadcast the key negotiation message: IDA|NA||MACK(IDA|NA). Node B receives this message from node A and vice-versa IDB|KB||MACK(IDB|NB). Finally shared session key is established as follows: KAB= MACK(NA|NB)

The drawbacks of BROSK include compromise of a single node will divulge the common key, an intruder having access to the master key could easily insert malicious nodes into the network and revocation of malicious nodes is very difficult.

Other related solutions Loop- Based Key Management Scheme [31] and Symmetric-Key Key Establishment adopted by Zigbee [32]

4.1.2. The full pairwise scheme:

Each of the n nodes in the network receives n-1 pairwise keys to communicate with every other node. There are a total of ${}^{n}C_2$ unique keys in the network. Nodes authenticate to the base station after which the base station sends a link key securely to both parties [33].

The advantages of the full pairwise scheme are high-security level, easy revocation of nodes due to perfect resilience and node-to-node authentication

However, this scheme faces the disadvantage of having a great memory overhead

4.1.3. Matrix-based Scheme

Efficient Pairwise Key Establishment and Management in Static WSN [34]: The first phase is the Setup Key Pre-Assignment Phase. In this, the KDS generates 220 distinct keys. Any key is randomly assigned to a node Ni. The KDS then assigns setup keys to each node under certain rules to ascertain that any two nodes have at least two keys in common (from the remaining keys). From the rest in the key pool (P) randomly η keys are selected and an mXn matrix is constructed, where ($m= \sqrt{\eta}$). Finally, K_{cij} is stored in the node's memory. Next phase is Common Keys Discovery Phase: Node ID and keychain ID are broadcasted to the neighbors. On receiving KC the receptor node searches for common keys.

i.e. N_a: kC12 ⟶ N_b: kC2

k1	k2
K3	K4

Nb: searches for kC12 or kC22

In the third Pairwise Key Computation Phase, each node establishes a private pairwise key which is unaware to other nodes. In the fourth Key Ring Establishment phase, only private pairwise keys (Na and Nb) and k_N are kept and other keys are removed keeping security in mind. However, greater processing and communication overheads pose a significant problem.

4.1.4. Blundo's Polynomial-based protocol [35]:

In this approach partially solved symmetric polynomials are generated by the KDC. These polynomials are symmetric and bivariate polynomials of degree't'. All the nodes are pre-loaded with these polynomials solved for their node coefficient. When two nodes intend to establish a secure communication path between them they broadcast their node identity and solve for the ID of their respective partner. Since the polynomial is symmetric both nodes end with the same value which, serves as the common key between them.

Example: $f(x,y) = 4x^2y^2 + x^3y^1 + x^1y^3 + 5$

It's asymmetric bivariate 3-degree polynomial

- STEP1: compute

$f(1,y) = 4y^2 + y^1 + y^3 + 5$

$f(2,y) = 16y^2 + 8y^1 + 2y^3 + 5$

- STEP2: The Setup server loads the sensor node with coefficients
- STEP3: Each sensor node broadcasts its own ID
- STEP4: Receiver uses ID to compute a shared secret key

$K_{uv} = f(u,v) = f(v,u) = K_{vu}$

$K_{12} = f(1,2) = 31 = f(2,1) = K_{21}$

The following figures provide a comparative analysis of various schemes based on different parameters**.**

Table 1: Summary of various schemes based on efficiency and flexibility parameters

Scheme	Node Authentication	Deployment Knowledge	Linkability	Bandwidth Utilization
BROSK	**No**	**No**	**No**	**$[b_k][b_k]$**
Full Pairwise	**Yes**	**No**	**No**	**$[1_{ID}][b_{ID}]$**
Blom's Scheme	**Yes**	**No**	**No**	**$[(\lambda+1)k][b(\lambda+1)k]$**
Blundo's Scheme	**Yes**	**No**	**No**	**$[1_{ID}][b_{ID}]$**
Q-Composite	**No**	**No**	**No**	**$[k_{ID}][bk_{ID}]$**
Combinatorial Design	**Yes**	**No**	**Yes**	**$[1_{ID}][b_{ID}]$**

4.2. Other Important schemes

4.2.1. SHELL [35]

This scheme works on the following assumptions: Until a compromised node is a neighbor of another compromised node, both these nodes won't know about the status of each other. The attacker does not launch a direct attack on a particular node as he is unaware of the content stored in the nodes.

The data structures used are as follows:

Command node: stores database of all node IDs. Then Ksg is the discovery key (pre-loaded in each sensor). There is also a one-way hash function to recomputed Ksg. KSCH and KSkey: preloaded for initial key distribution.'K' administrative keys and 'C' communication keys are set by a trade off between memory available for keying and bandwidth utilization.

The working of the scheme is as follows:

NETWORK BOOTSTRAPPING:

It is the first step when sensor nodes discover themselves and organize into clusters. It is in this phase only when gateways start communicating with each other.

GATEWAY REGISTRATION:

Gateways broadcast their IDs and location in encrypted form to the command node. Command node then establishes the one-way link-specific keys such that $K_{GIGJ} \neq K_{GJGI}$ (for gateway I and j respectively). Ksg is also sent to the gateway for establishing contacts with the sensors.

SENSOR DISCOVERY:

Sensors broadcast their ID and location encrypted by K_{sg} to the gateway. The gateway then decrypts the message. The sensor nodes now generate a new k_{id} by one way hash function. This hashed value is not known to the gateway (kind of security protocol adopted by the authors).

CLUSTERING:

Sensors need to be uniquely assigned to a particular gateway. Also, clustering spreads functionality of key management and hence prevents a single point of failure.

I. Initial key distribution:

The gateway distributes keys to all the sensors in its cluster using EBS-based scheme for key distribution. Factors such as Size of the cluster, Memory available in the sensor, Expected lifetime, Deployment terrain are taken into consideration while distributing keys: After all the analysis, the EBS- table along with a list of all the nodes is sent to the command node.

II. Assigning key- generating gateways:

Apart from the cluster head, the command node elects a number of nodes as a gateway (say 2) for generating keys. Let these gateways be $G_{k1}[i]$ and $G_{k2}[i]$. The command node sends a portion of the EBS matrix to $G_{k1}[i]$ and $G_{k2}[i]$ in such a way that these gateways are not aware of the keys a node receives from another gateway. This partitioning helps in preventing one gateway in manipulating the entire cluster in case of being compromised.

Based on all of the above information the command node issues K_{SCH} of all sensors in its cluster to the gateway and K_{Skey} to $G_{k1}[i]$ and $G_{k2}[i]$. The command node sends a portion of the EBS matrix to $G_{k1}[i]$ and $G_{k2}[i]$ in such a way that these gateways are not aware of the keys a node receives from another gateway. This partitioning helps in preventing one gateway in manipulating the entire cluster in case of being compromised. Based on all of the above information the command node issues KS_{ch} of all sensors in its cluster to the gateway & KS_{key} to $G_{k1}[i]$ and $G_{k2}[i]$.

The advantages of this scheme are as follows: Keys are periodically refreshed. The CH sends new communication keys to $G_{k1}[i]$ and $G_{k2}[i]$ for the same then the corresponding encryption and distribution process takes place all over again, secure in-network processing, attack/failure mitigation is possible, enhanced network survivability against node capture and collision-free algorithm.

The disadvantages are Latency during initial setup, SHELL does not handle the scenario where the compromised nodes communicate directly by a separate path set-up by the adversary.

4.2.2. THREE TIER SECURITY SCHEME IN WSN WITH MOBILE SINKS

In wireless sensor network collecting data from the sensor node is a complex process because the attacker can compromise the network easily. Q composite key pre-distribution techniques are used in existing techniques i.e. if the attacker is able to compromise a fraction of nodes then can compromise the network easily.

The authentication mechanism can be strengthened even further by introducing a three-tier security protocol. This framework can be implemented over any basic pairwise key pre-distribution scheme.

In the proposed scheme [36] two polynomials are used namely:

- Mobile polynomial pool: for the mobile sink to access the network
- Static polynomial pool: for pairwise key establishment between the nodes.

GENERAL DESCRIPTION OF THE SCHEME:

If sink wants to collect data from sensor node it will have to send the key to the sensor node from the mobile polynomial pool. This key is sent via the stationary access node to get access from the network. If this stationary access node finds the key to being correct then it sends it to the sensor node by selecting the key from the static polynomial pool. Sensor node verifies the keys in the static polynomial pools. If both keys are verified to be correct then the mobile sink, stationary access point, and the sensor nodes are not compromised. The sensor node sends the acknowledgment to the sink. After receiving the acknowledgment the sink sends key Kc to the sensor node. This key is used by the sensor node to encrypt the messages.

V. KEY DISTRIBUTION AND MANAGEMENT IN WBAN

The advent of e-health has revolutionized the whole healthcare domain. With the use of WSN we can monitor and track the well being of the in patients as well as the outpatients. This report discusses a brief overview of the WSN and its evolution in the healthcare domain, focusing on the security aspect of the medical information of the person transmitted. Due to the fear of the personal information being stolen or divulged people are not able to mentally trust this highly potential application of e-health. Since the channels used for transmission are public the data so transmitted is highly vulnerable to many cybersecurity attacks viz node compromise, eavesdropping, message delay, message replay etc. Therefore the report tries to highlight the already existing techniques to secure the communication and the fact that in order to avail the full benefits of e-health application new techniques for secure communication over public channels which do not resource greedy need to be developed.

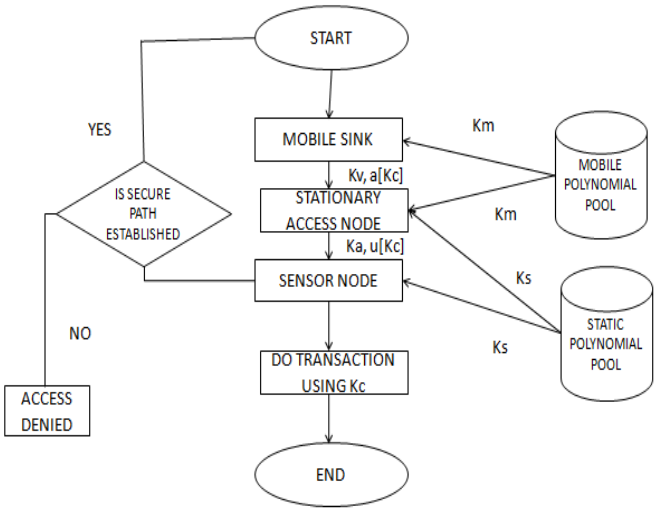


Figure 6: Flowchart of the three-tier security scheme

4.3. TinySec [37]

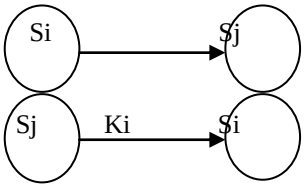
This is one of the most preliminary security schemes. It aims at providing link layer security and by encrypting and authenticating the information sent by the biosensors. There is a single group key which is shared by all the sensors in the network. All the data packets are fully encrypted and their MAC being calculated. Before the deployment of the sensors, the key is manually programmed into the sensors thereby, providing minimal security to the network as any captured key can easily reveal this shared group key.

4.4. A Hybrid Key Management Scheme for Healthcare Sensor Networks

This scheme proposed by D.P. Aggarwal et al [38] is hybrid key management scheme that uses a Merkel Hashtable for key distribution and shared key discovery. It involves two phases key distribution phase and shared key discovery phase. Γ acts as the gateway access point between the WBAN and the internet. It is capable of performing higher order functionalities. It contains Mprivate and Mpublic (private and public key of master), the key pool (P) and the hashed values of the keys.

Each node stores the following 5 identifiers: [Ni, Ki, h(Ki), M(public, h(Mpublic)]. Each node is assigned its node ID (Ni) and some keys from the key pool. These keys which are assigned from the key pool to specific nodes is called the node's key ring (Ki). Along with this nodes also receive Mpublic and its hashed value (h (m)). Whenever Si wants to establish a connection with the other node in the network it sends its identifier list. Sj checks for the common key and uses it to encrypt the information sensed by it.

Identifier list

1) 

2)

= [data, h(M), Φ(h(Ki))]

h(M) is used to verify that the information is received from a trusted source.

3) HBPi= [Ni, h(kx)©h(Kx+1)©h(Kx), h(M)]
Heart Beat Package helps prevent DOS attack by providing network retracability.

The result of all the possible values returned by χ is calculated and stored by the coordinator. Public key identifiers of all the key rings are XORed simultaneously and stored in the lookup table. Next, a challenge is broadcasted to the whole network. In response, each node sends its heartbeat packet to the coordinator. Node id and its hashed values are extracted by the coordinator from the reply. Finally if the h(M) value and the value stored in the lookup table match, the node is authenticated and trust is established.

Though several schemes exist to identify node compromise attacks and intrusion detection they are extremely resourced greedy. This calls for some quality research in developing new key distribution and intrusion detection algorithms that use as minimum energy as possible.

VI. CONCLUSION

In this paper, we have reviewed state of the art civilian applications of WSNs. these sensor networks provide an alternative style of living often termed as assisted living. Owing to this fact they find a number of applications in agriculture, smart living, smart parking, and e-health. Being highly potent in nature these sensor networks face a huge number of security threats. We have discussed the componenets of WSN [41], threats on WSN along with counteractive measures to combat these threats. As security mechanisms, many key distribution and management techniques have been proposed by authors both in WSN and WBAN. We have compared and contrasted these schemes on metrics suitable to WSNs.

5. REFERENCES

[1] Khan, Shafiullah, Al-Sakib Khan Pathan, and Nabil Ali Alrajeh, eds. *Wireless sensor networks: Current status and future trends*. CRC Press, 2016.

[2] Moghaddam, Mahta, Dara Entekhabi, Yuriy Goykhman, Ke Li, Mingyan Liu, Aditya Mahajan, Ashutosh Nayyar, David Shuman, and Demosthenis Teneketzis. "A wireless soil moisture smart sensor web using physics-based optimal control: Concept and initial demonstrations." *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing* 3, no. 4 (2010): 522-535.

[3] N.G. Shah, U.B. Desai, I. Das, S.N. Merchant, S.S. *Yadav In-field wireless sensor network (WSN) for estimating evapotranspiration and leaf wetness*Int. Agric. Eng. J., 18 (3–4) (2009), pp. 43-51

[4] Gutiérrez, Joaquín, Juan Francisco Villa-Medina, Alejandra Nieto-Garibay, and Miguel Ángel Porta-Gándara. "Automated irrigation system using a wireless sensor network and GPRS module." *IEEE transactions on instrumentation and measurement* 63, no. 1 (2014): 166-176.

[5] Díaz, Soledad Escolar, Jesús Carretero Pérez, Alejandro Calderón Mateos, Maria-Cristina Marinescu, and Borja Bergua Guerra. "A novel methodology for the monitoring of the agricultural production process based on wireless sensor networks." *Computers and electronics in agriculture* 76, no. 2 (2011): 252-265.

[6] Cambra, Carlos, Juan R. Díaz, and Jaime Lloret. "Deployment and performance study of an Ad Hoc network protocol for intelligent video sensing in precision agriculture." In *International Conference on Ad-Hoc Networks and Wireless*, pp. 165-175. Springer, Berlin, Heidelberg, 2014.

[7] Project Common Sense Net 2.0. EPFL Zurich and IISc Bangalore. <http://commonsensenet.in/>.

[8] Matese, A. D. G. S. F., S. F. Di Gennaro, A. Zaldei, L. Genesio, and F. P. Vaccari. "A wireless sensor network for precision viticulture: The NAV system." *Computers and electronics in agriculture* 69, no. 1 (2009): 51-58.

[9] Bhargava, Kriti, Arti Kashyap, and Timothy A. Gonsalves. "Wireless sensor network based advisory system for apple scab prevention." In *Communications (NCC), 2014 Twentieth National Conference on*, pp. 1-6. IEEE, 2014.

[10] Goncalves, Leandro Bertini Lara, Fausto Guzzo da Costa, Leandro Alves Neves, Jó Ueyama, Geraldo Francisco Donegá Zafalon, Carlos Montez, and Alex Sandro Roschildt Pinto. "Influence of mobility models in precision spray aided by wireless sensor networks." In *Journal of Physics: Conference Series*, vol. 574, no. 1, p. 012153. IOP Publishing, 2015.

[11] Voulodimos, Athanasios S., Charalampos Z. Patrikakis, Alexander B. Sideridis, Vasileios A. Ntafis, and Eftychia M. Xylouri. "A complete farm management system based on animal identification using RFID technology." *Computers and electronics in agriculture* 70, no. 2 (2010): 380-388.

[12] Malaver, Alexander, Nunzio Motta, Peter Corke, and Felipe Gonzalez. "Development and integration of a solar powered unmanned aerial vehicle and a wireless sensor network to monitor greenhouse gases." *Sensors* 15, no. 2 (2015): 4072-4096.

[13] Soliman, Hamdy, Komal Sudan, and Ashish Mishra. "A smart forest-fire early detection sensory system: Another approach of utilizing wireless sensor and neural networks." In *Sensors, 2010 IEEE*, pp. 1900-1904. IEEE, 2010.

[14] Das, Ipsita, C. P. R. G. Naveen, Shailendra S. Yadav, A. A. Kodilkar, N. G. Shah, S. N. Merchant, and U. B. Desai. "WSN monitoring of weather and crop parameters for possible disease risk evaluation for grape farms-sula vineyards, a case study." In *Proceedings of Conference on Geospatial Technologies and Applications, Geomatrix-2009, IIT Bombay, Mumbai*, pp. 27-29. 2009.

[15] Saha, Rajat, N. Raghuwanshi, S. Upadhyaya, W. Wallender, and D. Slaughter. "Water sensors with cellular system eliminate tail water drainage in alfalfa irrigation." *California Agriculture* 65, no. 4 (2011): 202-207.

[16] Barrenetxea, Guillermo, Francois Ingelrest, Gunnar Schaefer, and Martin Vetterli. "Wireless sensor networks for environmental monitoring: The sensorscope experience." In *Communications, 2008 IEEE International Zurich Seminar on*, pp. 98-101. IEEE, 2008.

[17] Hu, Fei, Laura Celentano, and Yang Xiao. "Error-resistant RFID-assisted wireless sensor networks for cardiac telehealthcare." *Wireless Communications and Mobile Computing* 9, no. 1 (2009): 85-101.

[18] Madigan, David, Wen-Hua Ju, P. Krishnan, A. S. Krishnakumar, and Ivan Zorych. "Location estimation in wireless networks: A Bayesian approach." *Statistica Sinica*(2006): 495-522.

[19] Lee, Jong-Hyouk, Byung-Jin Han, Hyung-Jin Lim, Yeong-Deok Kim, Navrati Saxena, and Tai-Myoung Chung. "Optimizing access point allocation using genetic algorithmic approach for smart home environments." *The Computer Journal* 52, no. 8 (2009): 938-949.

[20] Chen, Mingkai, and Tianhai Chang. "A parking guidance and information system based on wireless sensor network." In *Information and Automation (ICIA), 2011 IEEE International Conference on*, pp. 601-605. IEEE, 2011.

[21] Orski, K. "Best space scenario." *Traffic Technology International* (2003).

[22] Mouskos, Kyriacos, Maria Boile, and Neville Anthony Parker. *Technical solutions to overcrowded park and ride facilities*. No. FHWA-NJ-2007-011. New Jersey Department of Transportation, 2007.

[23] Männi, U. "Smart sensing and time of arrival based location detection in parking management services." In *Electronics Conference (BEC), 2010 12th Biennial Baltic*, pp. 213-214. IEEE, 2010.

[24] Serpen, Gursel, and Chao Dou. "Automated robotic parking systems: real-time, concurrent and multi-robot path planning in dynamic environments." *Applied Intelligence* 42, no. 2 (2015): 231-251.

[25] Chakraborty, Suryadip, Anagha Jamthe, Saibal K. Ghosh, and Dharma P. Agrawal. "From theory to application: Wireless monitoring of patients suffering from neurodegenerative diseases." In *Circuits and Systems (MWSCAS), 2013 IEEE 56th International Midwest Symposium on*, pp. 944-947. IEEE, 2013.

[27] Cheng, Ho Ting, and Weihua Zhuang. "Bluetooth-enabled in-home patient monitoring system: Early detection of Alzheimer's disease." *IEEE Wireless Communications* 17, no. 1 (2010).

[28] Chen, Min, Sergio Gonzalez, Victor Leung, Qian Zhang, and Ming Li. "A 2G-RFID-based e-healthcare system." *IEEE Wireless Communications* 17, no. 1 (2010).

[29] Puri, Sanjeev, and S. P. Tripathi. "Dynamic High Level Cross Layer Security Mechanisms for Wireless Sensor Networks." *International Journal of Information Technology and Computer Science (IJITCS)* 4, no. 6 (2012): 45-56.

[30] Lai, Bocheng, Sungha Kim, and Ingrid Verbauwhede. "Scalable session key construction protocol for wireless sensor networks." In *IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES)*, pp. 7. 2002.

[31] Zeng, YingZhi, BaoKang Zhao, JinShu Su, Xia Yan, and Zili Shao. "A loop-based key management scheme for wireless sensor networks." In *International Conference on Embedded and Ubiquitous Computing*, pp. 103-114. Springer, Berlin, Heidelberg, 2007.

[32] Alliance, ZigBee. "ZigBee Document 053474r06." *Version* 1 (2004): 14.

[33] Raazi, Syed Muhammad Khaliq-ur-Rahman, Heejo Lee, Sungyoung Lee, and Young-Koo Lee. "BARI: A distributed key management approach for wireless body area networks." In *Computational Intelligence and Security, 2009. CIS'09. International Conference on*, vol. 2, pp. 324-329. IEEE, 2009.

[34] Raazi, Syed Muhammad Khaliq-ur-Rahman, Heejo Lee, Sungyoung Lee, and Young-Koo Lee. "BARI: A distributed key management approach for wireless body area networks." In *Computational Intelligence and Security, 2009. CIS'09. International Conference on*, vol. 2, pp. 324-329. IEEE, 2009.

[35] Cheng, Yi, and Dharma P. Agrawal. "Efficient pairwise key establishment and management in static wireless sensor networks." In *Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on*, pp. 7-pp. IEEE, 2005

[36] Puri, Sanjeev, and S. P. Tripathi. "Dynamic High Level Cross Layer Security Mechanisms for Wireless Sensor Networks." *International Journal of Information Technology and Computer Science (IJITCS)* 4, no. 6 (2012): 45-56.

[37] Rasheed, Amar, and Rabi N. Mahapatra. "The three-tier security scheme in wireless sensor networks with mobile sinks." *IEEE Transactions on Parallel and Distributed Systems* 23, no. 5 (2016): 958-965.

[38] H. S., Sim, M. L., and Tan, C. M., Security issues of wireless sensor networks in healthcare applications. BT Technol. J. 24(2):138–144, 2006

[39] Karlof, Chris, Naveen Sastry, and David Wagner. "TinySec: a link layer security architecture for wireless sensor networks." In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pp. 162-175. ACM, 2004.

[40] Meharia, Pallavi, and Dharma P. Agrawal. "A hybrid key management scheme for healthcare sensor networks." In *Communications (ICC), 2016 IEEE International Conference on*, pp. 1-6. IEEE, 2016

[41] Sharma, Shamneesh, Dinesh Kumar, and Keshav Kishore. "Wireless Sensor Networks-A review on topologies and node Architecture." *International Journal of Computer Sciences and Engineering* 1, no. 2 (2013): 19-25.

