International Journal of Recent Academic Research
Vol. 01, Issue 05, pp.159-164, August, 2019
Available online at http://www.journalijrar.com

RESEARCH ARTICLE

A REVIEW ON SECURITY ISSUES IN WIRELESS SENSOR NETWORKS

***Aliyu Musa Bade and Adamu Abdullahi Garba**

Department of Computer Science, Yobe State University Damaturu, Nigeria

ARTICLE INFO

Article History:
Received 20th May 2019,
Received in revised form
17th June 2019,
Accepted 14th July 2019,
Published online
21st August 2019.

ABSTRACT

With increasing dependency on technology, Wireless Sensor Networks (WSNs) had gained more and more popularity in the areas of communication, sensing and computing among investors as well as researchers over the years. The proceeds had since been able to simplify complexity in sensing networks, revealing previously unnoticed observable facts. Major research activities being carried out in this field includes deployment, localization, synchronization, architecture, middleware, security, designing less power consuming devices, abstractions and higher level algorithms for sensor specific issues. However, WSN designs still exhibits security issues in their applications that are of concern. This paper explains a synopsis of ongoing research activities, various security problems involved in wireless sensor networks and possible solutions. The paper also reviewed into the various types of successful attacks carried out on these devices to provide future researchers with clues on how to improve their designs.

Key Words: Wireless Sensor Networks (WSN), Data Confidentiality, Sinkhole attack, Sybil Attack and Flooding Attack.

INTRODUCTION

Wireless sensor networks (WSNs) have fascinated a many researchers for it usage in serious applications. Some of the rich domains for active research provided by WSNs include networking, hardware and system design, distributed algorithm, software design models, data management, security and social factors (Pathan *et al.,* 2006; Culler and Hong, 2004). The idea of sensor network according to (Pathan *et al.,* 2006), is to scatter tiny sensing devices; which are proficient of sensing some changes of incidents/parameters and collaborating with further devices, over a explicit topographical area for some precise resolutions like target tracking, surveillance, environmental monitoring etc.

A Review on Wireless Sensor Network Architecture

Wireless sensor network (WSN) are diverse system comprising many small devices called nodes and actuators with general-purpose computing element. WSN network contains hundreds of low cost, low power and self-organizing node which are disseminated inside or narrowly to the system (Hiremani and Madne). In WSN, nodes involve of three main components-sensing, data processing and communication and another two constituents called aggregation and base station. An aggregation collects all the information from the neighboring nodes and forwards it to the based station for data processing. According to (Pathak *et al.*), WSN comprises of circulated self-organizing sensor to monitor physical or environmental condition. It consists of a collection of sensors where each sensor includes a radio, transceiver, antenna and microcontroller. The most important node in WSN is the Sink node; it's the base station where all other nodes in the network forward their packages to for further processing and transmission to the main station.

****Corresponding author:*** **Aliyu Musa Bade**

Sink node have additional computational power, memory and battery life and it acts as intermediary between the nodes and the main station. Figure 1 shows the architecture of a Wireless Sensor Network organization which comprises of the standard machineries like sensor nodes (sink/actuator), gateways, internet, and satellite link. Many algorithms have been constructed for wireless sensor networks that are custom-made to meet their processing and communication needs. PADS, SOWSN, RC5 algorithms, and an algorithm used for Indoor Location System (ILS) are few of the algorithms used by these networks. Practical algorithms like PADS are being designed to address the issue of data security while others like PC5 and SPINS are application driven perspective to support data integrity and confidentiality through encryption and keyed one-way hash function. Security is also achieved by: not agreeing replay of transmitted alerts, not authorizing Denial-of-Service attacks achieved by malicious nodes, not allowing imitation attacks to succeed through the use of applications like SOWSN (Burgner and Wahsheh, 2011). Paradells *et al.* (2009) used an algorithm that takes into account time and signal strength to obtain accurate localization. This is used for an ILS, which relies on signal strength (in terms of Received Signal Strength Indication or RSSI) and Time of Arrival/Time Difference of Arrival (TOA/TDOA). Synthesis tool called FABRIC is implemented as middleware application where support for wireless sensor networks application development is added through the generation of custom-tailored instances for target platforms. Routing and sensor data structures are defined with them being attached to the data type definitions that are represented as domains.

Application of Wireless Sensor Network

The main goal for WSN is to gather information from the physical world, wireless sensor network can work in almost any environment, specially where wired network is impossible to implement like under the oceans, desert and battle field.

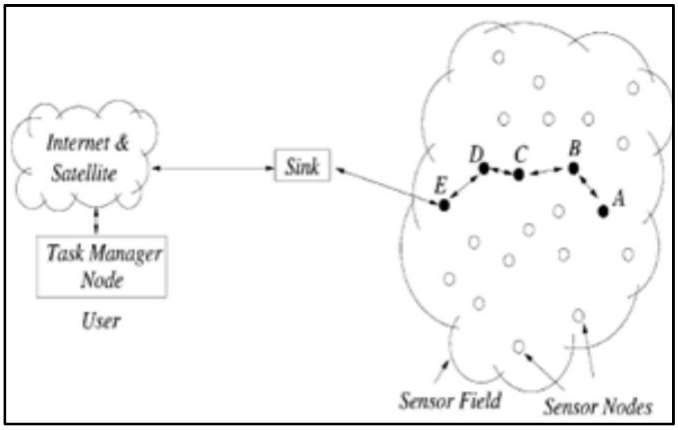

Figure 1. WSN Communication Architecture

The applications of WSN are diverse, its mainly involve in some kind of observing, tracing, or controlling specific applications that consists of habitat checking, smart grid, nuclear reactor control or fire detection. Its sensor consists of magnetic, thermal, visual, seismic, infrared and radar which helps to monitor a wide variety of conditions etc (Wang *et al.,* 2010; Prathap *et al.,* 2012; Al Ameen *et al.,* 2012). This section will highlight few important applications of WSN.

a) **Environmental monitoring:** environmental application of WSN includes forest fire detection, landside detection, air pollution detection and flood detection. So also in tracking the movement of animals, monitoring crops and felicitating irrigation.

b) **Vehicle detection**: WSN can also be used with a range of different sensors to detect the presence of vehicles in a particular geographical location.

c) **Health application**: sensors network provides edges for the incapacitated, integrated patient monitoring, diagnostic, drug administration in hospital, and also checking the movements and internal process of insects or other small animals etc.

d) **Industrial applications**: WSNs are commonly used in industries, in places like machinery condition-based maintenance. Some inaccessible locations are now accessible using sensor. Moreover, they can be used in measuring, monitoring of water levels within all ground etc.

e) **Military applications**: WSN are used in military situation awareness. Like in sensing enemies based locations, detection of enemy units' movements either on land or sea, detection of chemical threat. Likewise in Battled field surveillances, command control communications and targeting system.

f) **Other applications:** WSN can now be found in almost every new technology invented recently, like vacuum cleaners, micro-wave ovens. Other commercial application includes monitoring product quality, managing inventory and many more

This paper comprises of five main sections: Section I introduces the concept of WSN, Section II highlights the security requirement, Section III reviews the existing security issues in WSN, while Section IV discuses existing solutions to these security issues and the last section i.e. section V, is the conclusion.

Security requirement

Security in WSNs should be of prime concern because most of these sensor networks possess various mission-critical tasks and therefore they need security.

Security goals: The purpose for which security measures are employed in sensor networks can be classified into primary and secondary security goals. According to (Yu *et al.,* 2012), the primary goals are the standard security goals which cover the integrity, confidentiality, availability and authentication of the network and its resources, while the secondary goals cover the time localization, data freshness, self-organization and time synchronization. (Yu *et al.,* 2012) gave the description of both the primary and secondary goals below.

1. **Data Confidentiality:** this is the most important goal which provides that a sensor node hide its data contents to its neighbor. Therefore it's the ability of the network to conceal information or message from an unauthorized person or passive attacker hence ensuring confidentiality of the sensor network.

2. **Data Integrity:** When a malicious node present in the network injects false data or unstable conditions due to wireless station, it causes damage or loss of data hence the data integrity is compromised. Therefore a sensor network should ensure the reliability of data by making sure it's not altered or changed.

3. **Availability**: This is the primary importance for maintaining an operational network. It is to ensure the nodes are able to use the resources at any given time or that the network is always available for message to communicate.

4. **Authentication:** This is the ability to identify the origin of a message thereby ensuring the reliability of the information.

5. **Self-Organizing:** This is to ensure that every sensor node in the ad hoc network is self-governing and elastic enough to be self-organizing and self-healing according to unlike situations.

6. **Time Synchronization:** Sensors may wish to calculate the end to end delay of a packet as it travels between two pair wise sensors. A more cooperative sensor network may need group synchronization for following applications.

7. **Secure Localization:** A sensor network designed to locate errors will need accurate place information in order to pin point the location of a liability.

Constraints in WSNs

However, several restrictions such as low capability of computation, small memory or storage capacity, limited resources of energy, limited communication bandwidth because of restricted power and size of the sensor nodes and the unreliable channels employ communication in using WSNs

can cause difficulty in use of security and protection in WSNs (Kumar *et al.*). Data collection over wireless sensor networks does not trust in enthusiastic infrastructure. In several situations, the number of nodes responding a question is not distinguished before the data aggregation is directed (Ahmad Salehi *et al.,* 2013). Resource restricted portable devices are not able to provide heavily computation and communication load. WSNs are wireless network; therefore they are open and prone to various types of attack which can be active or non-active in nature. Because of high mobility nature of nodes network topology always gets changed, therefore it became a challenge for security systems when it comes to preventing malevolent attacks inside the ever changing dynamic network. A sensor network is a distributed network lacking a central management point. This may raise the strength of the sensor network. If in the case where the network is designed faultily then it can cause problems and it will be really difficult to handle the network (Sunitha and Chandrakanth, 2012). So a central management can help solve this problem. Preparing effective data aggregation, while protecting privacy and integrity is a difficult task in WSNs due to trust management, unreliable communication, unattended operations and other security challenges. Researchers like (Younis *et al.,* 2014) and (Teymourzadeh *et al.,* 2013) argued that sometimes it is stiff to straight use the formal security technique in WSNs due to these restrictions. It is essential to be attentive of the restrictions of sensor nodes for optimization the routine security algorithms in WSNs. Some limitations are in uniting security into a WSN like storage restriction, communication, computation, and processing capabilities .Comprehension of these restrictions and attaining suitable performance with security measures to address the necessities of an application are requirements in security protocols of designing need.

Security in WSN

This section will review security related issues in WSNs based on two parts; the threats to the layers of the sensor network and the various successful attacks that have been lunched on WSNs.

Threats to WSN layers: Wireless sensor networks employ layered architecture such as wired network architecture. This section will review the function of all the security layers in WSN and possible threat to each as explained by (Teymourzadeh *et al.,* 2013; Dhaye and Pande).

a) **Physical Layer:** The physical layer is liable for frequency collection, carrier frequency generation, signal detection, modulation, and data encryption. As with any radio-based medium, there exists the possibility of jamming attack in WSNs. Jamming is a type of attack which inhibits with the radio frequencies that a network's nodes are consuming. Here the enemy has the potential to interrupt the network provided the jamming sources are erratically disseminated in the network. *Tampering* is another threat to the physical layer where the adversary extracts sensitive information such as cryptographic keys or other data on the node

b) **Data Link Layer:** The data link layer is liable for the multiplexing of data streams, data frame detection and error control. It ensures reliable point-to-point and point-to-multipoint networks in a communication network. An adversary may strategically use *Collision* attack on precise packets such as ACK control messages. A possible result of such collisions is the costly exponential back-off in certain media access control (MAC) protocols. *Exhaustion* is another threat to link layer where adversary can use repeated collision to cause resource exhaustion. Instead of stopping access to a service outright, an attacker can degrade it in order to gain an advantage such as causing other nodes in a real-time MAC protocol to miss their broadcast deadline

c) **Network Layer:** Providing the best path for effective routing technique is the aim of Network layer. Routing the data from node to node, node to sink, node to base station, node to cluster head and vice versa are in charge of this layer. ID based protocols and data centric protocols are used by WSN for routing mechanism. The injection of malicious routing information into the network is one of the simplest attacks which results in routing inconsistencies. Here some routing protocols are susceptible to replay by the attacker of legitimate routing messages.

d) **Transport Layer:** The transport layer is responsible for managing end-to-end connections. When a protocol is required to preserve state at either end of a connection it becomes susceptible to memory exhaustion through *flooding*. An attacker may recurrently make new connection requests until the resources required by each connection are exhausted or reached a maximum limit. In either case, further legitimate requests will be ignored. Disruption of an existing connection in WSN is another threat and is referred to as *Desynchronization.*

e) **Application Layer:** Application Layer use to display ultimate yield by guarantee smooth information flow to lower layers. This layer is in charge of data collection, management and processing of the data by using the application software to obtain trustworthy consequences. An adversary may attempt to disrupt the network's operation by broadcasting a high-energy signal. If the transmission is powerful enough, the entire system's communication could be jammed.

More sophisticated attacks are also possible; the adversary might inhibit communication by violating the 802.11 medium access control (MAC) protocol by, say, transmitting while a neighbour is also transmitting or by incessantly requesting channel access with a request-to send signal

Attacks on WSN: A researcher (Pathan *et al.,* 2006) argued that attacks against wireless sensor networks are of two different levels of views, attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). Furthermore, WSNs are vulnerable to security attacks due to the broadcast nature of the transmission medium. According to these attacks are broadly classified in two categories i.e. active attacks and passive attacks. This section points out these various attacks on wireless sensor networks as described by (Pathan *et al.,* 2006; Younis *et al.,* 2014; Teymourzadeh *et al.,* 2013).

A. Passive Attacks: Passing attacks can be regarded as the monitoring and listening of the communication channel by

unauthorized attackers. Below are common attacks against sensor privacy.

- **Traffic Analysis:** Even when the messages relocated are encoded, it still leaves a high option analysis of the communication patterns. Sensor activities can possibly reveal many information to permit an adversary to cause cruel harm to the sensor network.
- **Camouflage adversaries:** One can enclosure their node to hide in the sensor network. After that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.
- **Monitor and Eavesdropping**: This is the most common attack to privacy. By snooping to the data, the adversary could easily discover the communication contents.

B. Active Attacks: When an unsanctioned attacker monitors, listens to and alters the data stream in the communication channel, its known as active attack. The following attacks are active in nature.

- **Selective Forwarding:** A malicious node can selectively drop only certain packets. Especially effective if combined with an attack that gathers much traffic via the node. In sensor networks it is assumed that nodes faithfully forward received messages. But some compromised node might refuse to forward packets, however neighbors might start using another route.
- **Black hole/Sinkhole Attack:** In this attack, a malicious node acts as a black hole to attract all the traffic in the sensor network. In fact, this attack can affect even the nodes of those are considerably far from the base stations.
- **Routing Attacks:** The attacks which acts on the network layer are called routing attack. The following are the attacks that happen while routing the messages.
- **Node Subversion:** Capture of a node may reveal its information including disclosure of cryptographic keys and thus compromise the whole sensor network. A particular sensor might be captured, and information (key) stored on it might be obtained by an adversary.
- **False Node:** A false node involves the addition of a node by an adversary and causes the injection of malicious data. An intruder might add a node to the system that feeds false data or prevents the passage of true data. Insertion of malicious node is one of the most dangerous attacks that can occur
- **Passive Information Gathering**: An adversary with powerful resources can collect information from the sensor networks if it is not encrypted. To minimize the threats of passive information gathering, strong encryption techniques needs to be used.
- **Wormholes Attack**: Wormhole attack is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location.

Some researchers categorized these attacks based on the affected layer of the network. Table 1 exhibits the various attacks categorized under which layer it was carried on.

A review on existing security solutions

According to (Zhao, 2012), WSN is vulnerable to node capture attacks in which an attacker can capture one or more sensor nodes and reveal all stored security information which enables him to compromise a part of the WSN communications. The authors proposed an efficient key management scheme in EECBKM through the use of the pair wise keys between sensor nodes. Thus it reduces the impact of node capture attacks, consumes less energy, increases the strength to communication denial of service and generally improves secure routing. As explained by (Sekhar and Sarvabhatla, 2012), the security of WSNs can be improved through

Table 1. Layers Attacks on WSNs

Network Layers	Physical	Data Link	Network and routing	Transport
Attacks	Jamming			
Defence	Spread-spectrum, priority messages	____	_____	_____

Network Layers	Attacks	Defence
Physical layer	Jamming	Spread-spectrum and priority message
	Tampering	Tamper-proofing, hiding
Data Link layer	Collision	Error-correcting code
	Exhaustion	Rate limit
	Unfairness	Small frames
Network and Routing layer	Black holes	Authorization
		Monitoring, redundancy
	Hello Flood	Authentication, packet
		Leashes by using geographic and temporal
Transport layer	Spoofed Routing	Egress filtering
		Authentication, monitoring
	Information and selective forwarding	Authentication, monitoring
	Sybil attack	Authentication, monitoring
	Sinkhole	Redundancy
		Client puzzles, Rate limitation

Table 1. A Summary of Schemes in Wireless Sensor Network

Security Schemes	Attacks	Network Architecture	Major Features
JAM	DoS Attack (Jamming)	Traditional wireless sensor network	Avoidance of jammed region by using coalesced neighbour nodes
TIK	Wormhole Attack, Information or Data Spoofing	Traditional wireless sensor network	Based on symmetric cryptography, Requires accurate time synchronization between all communicating parties, implements temporal leashes
Random Key Predistribution	Data and information spoofing, Attacks in information in Transit	Traditional wireless sensor network	Provide resilience of the network, Protect the network even if part of the network is compromised, Provide authentication measures for sensor nodes
Statistical En-Route Filtering	Information Spoofing	Large number of sensors, highly dense wireless sensor network	Detects and drops false reports during forwarding process
Radio Resource Testing, Random Key Pre-distribution	Sybil Attack	Traditional wireless sensor network	Uses radio resource, Random key pre-distribution, Registration procedure, Position verification and Code attestation for detecting sybil entity
Bidirectional Verification, Multi-path multi-base station routing	Hello Flood Attack	Traditional wireless sensor network	Adopts probabilistic secret sharing, Uses bidirectional verification and multi-path multi-base station routing
On Communication Security	Information or Data Spoofing	Traditional wireless sensor network	Efficient resource management, Protects the network even if part of the network is compromised
REWARD	Blackhole attacks	Traditional wireless sensor network	Uses geographic routing, Takes advantage of the broadcast inter-radio behaviour to watch neighbour transmissions and detect blackhole attacks
Tiny Sec	Data and Information spoofing, Message Replay Attack	Traditional wireless sensor network	Focuses on providing message authenticity, integrity and confidentiality, Works in the link layer
SNEP & μTESLA	Data and Information Spoofing, Message Replay Attacks	Traditional wireless sensor network	Semantic security, Data authentication, Replay protection, Weak freshness, Low communication overhead
Wormhole based	DoS Attack (Jamming)	Hybrid (mainly wireless partly wired) sensor network	Uses wormholes to avoid jamming

protected grouping. As sensor nodes are required to bind themselves in order to complete a particular task it is important that the group members communicate securely between each other, despite the fact that overall security may also be in use. Here the more powerful nodes are mostly in charge of protecting members of static group. Data traffic in WSN network is a significant trouble as the data transfer increases. (Du and Li, 2011) Proposed Secure Data Aggregation as a security solution where such data is particularly enticing to an attacker. The main aim in this area is to use resilient functions that will be able to discover and report forged reports through demonstrating the authenticity of data. The implementation of the 802.15.4 standard, a security suite that provides link layer security services, is another security solution in WSNs (Jain *et al.,* 2012). It offers security services in access control, data encryption, frame integrity and sequential freshness. The 802.15.4 security suites are implemented on the radio chips where all the necessary cryptographic computations are performed in hardware, thus reducing energy consumption. MiniSec (Healy *et al.,* 2009), a secure network layer protocol is another security solution in WSNs. It uses offset codebook (OCB) mode as its block cipher mode of operation, which offers authenticated encryption with only one pass over the message data. Even though MiniSec still requires some work, especially in terms of implementation details, it has provided energy efficient security to WSNs. Another security solution as introduced by (Luk *et al.,* 2007) is Sizzle, a secure web server designed to run on sensor mote class devices and is the first end-to-end security architecture for WSNs. Generally, Sizzle offers a very impressive code size, memory usage and speed for the services it provides. Over the years various holistic approaches (Perrig *et al.,* 2002) aimed at improving the performance of wireless sensor networks with respect to security, longevity and connectivity under changing environmental conditions have been proposed and/or implemented. Today different schemes addresses different security issues in WSNs ranging from secure routine, secure distributed sensor network, mapping protocol, prevent jamming, encryption protocol etc. below is a table that depicts more of these schemes and their features.

Conclusion

Security related issues in wireless sensor network have become an important part of research in present developments. This research paper reviewed the technology of WSN and the various security requirements in Wireless sensor networks. The Various security issues/attacks has been investigated and reviewed. Some of the existing security solutions and the security challenges help solved were reviewed to provide feature researchers with clues as to where to improve them.

REFERENCES

Ahmad Salehi, S., *et al.* 2013. Security in Wireless Sensor Networks: Issues and Challenges in Space Science and Communication (IconSpace), IEEE International Conference on. 2013. IEEE.

Al Ameen, M., Liu, J. and Kwak, K. 2012/ Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of medical systems,* 36(1): p. 93-101.

Burgner, D.E. and Wahsheh, L.A. 2011. Security of wireless sensor networks in Information Technology: New Generations (ITNG), Eighth International Conference on. 2011. IEEE.

Culler, D.E. and Hong, W. 2004. Wireless sensor networks. Communications of the ACM, 47(6).

Dhaye, M. and Pande, H. Security in Wireless Sensor Networks: Issues and Challenges.

Du, J. and Li, J. 2011. A Study of Security Routing Protocol for Wireless Sensor Network. in Instrumentation, Measurement, Computer, Communication and Control, First International Conference on. 2011. IEEE.

Gupta, V., *et al.,* 2005. Sizzle: A standards-based end-to-end security architecture for the embedded internet. *Pervasive and Mobile Computing,* 1(4): p. 425-445.

Halim, T. and Islam, M.R. 2012. A study on the security issues in WSN. *International Journal of Computer Applications,* 53(1): p. 26.

Healy, M., Newe, T. and Lewis, E. 2009. Security for wireless sensor networks: A review in Sensors Applications Symposium, SAS 2009. IEEE. 2009. IEEE.

Hiremani, V. and Madne, M. Secure Mechanism for Wireless Sensor Networks-A Review.

Jain, A., Kant, K. and Tripathy, M. 2012. Security solutions for wireless sensor networks in Advanced Computing & Communication Technologies (ACCT), Second International Conference on. 2012. IEEE.

Karlof, C., Sastry, N. and Wagner, D. 2004. TinySec: a link layer security architecture for wireless sensor networks in Proceedings of the 2nd international conference on Embedded networked sensor systems, ACM.

Kim, J. and Kim, K. 2013. A scalable and robust hierarchical key establishment for mission-critical applications over sensor networks. *Telecommunication Systems,* 52(2): p. 1377-1388.

Kumar, N., *et al.,* Detecting Wormhole Attacks on Wireless Ad-hoc Networks: A Group based Approach.

Kumar, V., Jain, A. and Barwal, P. Wireless Sensor Networks: Security Issues, Challenges and Solutions.

Lalitha, T. and Devi, A.J. 2014. Security in Wireless Sensor Networks: Key Management Module in EECBKM in Computing and Communication Technologies (WCCCT), World Congress on. 2014. IEEE.

Luk, M., *et al.* 2007. MiniSec: a secure sensor network communication architecture. in Proceedings of the 6th international conference on Information processing in sensor networks, ACM.

Newsome, J., *et al.* 2004. The sybil attack in sensor networks: analysis & defenses in Proceedings of the 3rd international symposium on Information processing in sensor networks. ACM.

Panic, G., *et al.* 2012. Design of a sensor node crypto processor for ieee 802.15. 4 applications in SOC Conference (SOCC), IEEE International. 2012. IEEE.

Paradells, J., Vilaseca, J. and Casademont, J. 2009. Improving security applications using indoor location systems on wireless sensor networks in Proceedings of the International Conference on Advances in Computing, Communication and Control, ACM.

Pathak, S., Chawla, K. and Aggarwal, H. Improved Secure Routing Scheme in WSN.

Pathan, A., Lee, H.W. and Hong, C.S. 2006. Security in wireless sensor networks: issues and challenges in Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference, IEEE.

Perrig, A., *et al.,* 2002. SPINS: Security protocols for sensor networks. Wireless networks, 8(5): p. 521-534.

Prathap, U. *et al.* 2012. Wireless sensor networks applications and routing protocols: survey and research challenges in Cloud and Services Computing (ISCOS), International Symposium on. 2012. IEEE.

Sekhar, V.C. and Sarvabhatla, M. 2012. Security in wireless sensor networks with public key techniques. in Computer Communication and Informatics (ICCCI), 2012 International Conference on. 2012. IEEE.

Sharma, D. 2014. Low cost enabled deployment of large amounts of sensor nodes.

Singh, S.K., Singh, M. and Singh, D. 2011. A survey on network security and attack defense mechanism for wireless sensor networks. *Int. J. Comput. Trends Tech.,* p. 5-6.

Strikos, A.A. 2007. A full approach for intrusion detection in wireless sensor networks. School of Information and Communication Technology.

Sunitha, K. and Chandrakanth, H. 2012. A Survey on Security Attacks in Wireless Sensor Network. International Journal of Engineering Research and Applications (IJERA), 2(4): p. 1684-1691.

Teymourzadeh, M., *et al.* 2013. Security in Wireless Sensor Networks: Issues and Challenges. *International Journal of Computer Networks & Communications Security,* 1(7).

Wang, Y., Lin, W. and Zhang, T. 2010. Study on security of wireless sensor networks in smart grid in Power System Technology (POWERCON), International Conference on. 2010. IEEE.

Ye, F., *et al.,* 2005. Statistical en-route filtering of injected false data in sensor networks. Selected Areas in Communications, IEEE Journal on, 2005. 23(4): p. 839-850.

Younis, M., *et al.* 2014. Topology management techniques for tolerating node failures in wireless sensor networks: A survey. *Computer Networks,* 58: p. 254-283.

Yu, Y. *et al.* 2012. Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. *Journal of Network and Computer Applications,* 35(3): p. 867-880.

Zhao, X. 2012. The security problem in Wireless Sensor Networks in Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on. 2012. IEEE.

****