International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

*Review Article*

# Review on Security Issues in Wireless Sensor Networks

**Heena Chawla*, Hardeep Kaur and Charanvir Kaur**

Department of Electronics Technology, Guru Nanak Dev University, Amritsar, India

Accepted 01 June 2016, Available online 07 June 2016, **Vol.6, No.3 (June 2016)**

***Abstract***

*Wireless Sensor Networks consist of a large number of pocket- sized sensors deployed in autonomous manner in the area under surveillance. These sensor networks are used in sensitive, unattended and remote environment. They have a wide range of applications and are used in almost every field like agriculture, industry, public safety and health services. They are used to gain knowledge about various parameters like temperature, vibrations, motion etc. in the area. The cost of establishment and maintenance of these networks is reasonable. These sensor networks face many challenges due to the use of wireless medium for communication which is prone to various types of attacks. There are various issues like energy exhaustion, memory and storage shortage, security attacks. It is very important to safeguard the network from attacks. Attacks result in loss of information and there is a cutback in number of bits transferred per second that is the throughput of the network reduces. This paper discusses the security requirements, security attacks and countermeasures against the attacks.*

***Keywords***: *Wireless Sensor Networks (WSNs); Security requirements and Security attacks*

## 1. Introduction

Wireless sensor network (WSN) is made up of a large number of minute sized sensors. The assembly of network consists of sensing entity, computing and processing entity and wireless communication entity. There are two types of motes- sink mote and the sensor motes. The sink node is also called base station. It instructs the sensor nodes about the type of data to be collected from the area under surveillance. The sensing unit of WSN which consists of the sensor nodes gathers the information and reports back to the sink node. The storage and processing of data takes place in the computing unit. The transmission of data occurs through multiple hops and RF band is used for communication (Kaplantzis *et al*, 2007). The assembly of WSN is shown in Fig 1 and applications in Fig 2.

### *1.1 Characteristics of WSNs*

- WSNs are application specific and collect real time data.
- They perform specialized task as per the demand of the application.
- They are limited in terms of energy, power and battery life.
- Their installation and maintenance cost is less.
- They are influenced by noisy environment and are susceptible to various types of attacks (Ghildiyal *et al*).

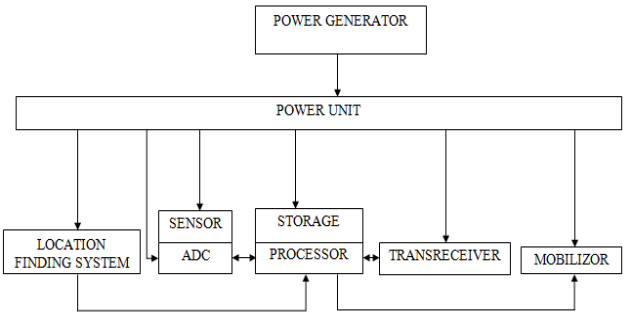


**Fig. 1:** Architecture of Wireless Sensor Networks

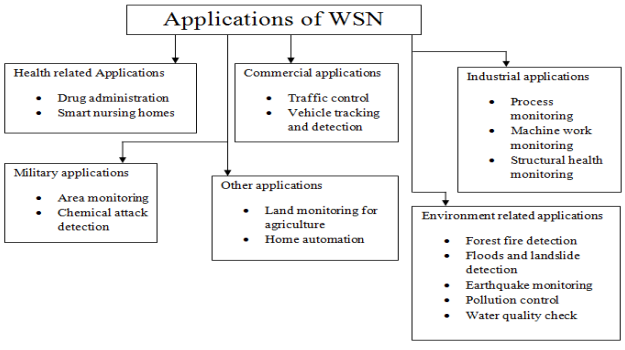


**Fig. 2:** Applications of Wireless Sensor Networks

*Corresponding author: **Heena Chawla**

*1.2 WSN Challenges*

- *Energy constraint*-Energy limitation is a major concern in WSNs. As the sensor networks are deployed in remote areas where recharging of batteries is not feasible so the energy of nodes decrease; thus affecting the functionality of the network.
- Network lifetime needs to be enhanced for prolonged functioning of the network. To achieve this goal the energy consumption should be minimized. Protocols used must be energy efficient. A lot of progress is needed in this area (Shio Kumar *et al*, 2010).
- *Topological changes*-Topology of WSN is dynamic. This is because the faulty nodes are removed and new sensor nodes are added to the network from time to time; the connections among the nodes are re-established. So routing protocols must keep in view the dynamic topology of the network to get accurate real-time information.
- *Hostile environment*-Another problem is the difficulty of surviving in the hostile environment. The nodes are susceptible to failures and can be physical tempered. Other hardware components can be destroyed; thus resulting in network failure. It is very difficult for WSN to survive in remote areas.
- *Security issues*-WSN is vulnerable to various attacks. The different layers of OSI are prone to different attacks. These attacks are a major threat to the integrity and confidentiality of the data. Information can be altered by the attacker; it can reach the unauthorized user; false information can be sent to the legitimate user or the legitimate user can be denied the access to data.
- *Memory constraint*-WSNs are limited in terms of memory. Flash memory and RAM are used in these networks. Storage capacity is not enough and needs to be enhanced for better performance (Shio Kumar *et al*, 2010).

## 2. Security goals

For reliable and secure communication the network must ensure the fulfillment of following security requirements.

- *Data Confidentiality*: Data should not be disclosed to any third-party. Secrecy of the information should be maintained. Unauthorized users should not be able to overhear the information. It should be ensured that information is concealed from the attackers.
- *Data Integrity*: For secure and reliable communication, data received at the destination node must be same as that sent by the source node. The intermediate nodes must not change the information contained in the packets. Malicious activity should not corrupt the data (Modares *et al*, 2011).
- *Data Authentication*: The attacker can not only alter the information contained in the packets but can also introduce fallacious packets in the network. So verification of sender and receiver identities needs to be carried out as a defensive step against the action of any malicious activity. Data authentication is challenging for WSNs as they are deployed in remote areas where it is very difficult to verify the identity of the sender. Only the authorized users should be able to access the information and the illegitimate users should be denied the access (Modares *et al*, 2011; Padmavathi *et al* , 2009).
- *Data Availability*: Availability of data is very vital for proper functioning of the network. Services of the network should be available whenever necessary. Users should be able to use the resources whenever they intend to (Kavitha *et al*, 2012).
- *Data Freshness*: Data freshness implies that the information received is current and up-to-date. The previous data should not be repeated that is real-time computation must be done. Security protocols must be able to detect and discard the duplicate messages (Padmavathi *et al*, 2009).

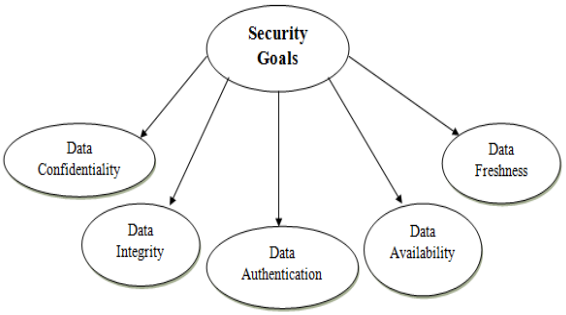


**Fig. 3**: Security goals for reliable communication

## 3. Attacks in WSNs

Different layers of OSI are prone to different attacks. The attacks can be classified into passive attacks and active attacks. Passive attacker snoops into the network and overhears the contents. Monitoring and Eavesdropping is the most common feature of passive attacks. They eavesdrop the information i.e. the data confidentiality is lost. They are difficult to detect as they are silent and don't make their presence felt. Passive intrusion doesn't hinder the operation of the network (Modares *et al*, 2011). Active attacker alters the message and obstructs the secure and reliable communication. It may harm the network in different ways. It can hinder the performance by not delivering the packets to the authorized and intended user or can mislead the destination node by introducing fallacious packets. Illegitimate user can gain the access to the confidential data and misuse it. A false node can be introduced by the attacker. This node is called malicious or compromised node. This node can alter

the message contents; thereby violating the data integrity principle. Wormhole attack, blackhole attack and denial of service attack are some of the active attacks (K. Das. *et al*, 2007; Padmavathi *et al*, 2009). Some of the attacks are explained as follows:

### *3.1. Jamming*

An eminent attack on physical layer of wireless networks is 'Jamming' attack that hampers with the radio frequencies used by the network nodes. In case of single frequency transmission, the attack is effective and it disrupts the network. The adversary starts communicating at same RF frequency as that of the network and causes unnecessary energy consumption by inserting intrusive malicious packets. Thus the network is jammed by the unwanted false packets and during this energy of nodes is consumed. Nodes must follow tactics against these attacks such as they should stop communication which means stop forwarding packets and switch to sleep mode during jamming phase and wake up when jamming period ends (Modares *et al*, 2011; Maróti *et al*, 2012).

### *3.2. Tampering*

In tampering, attacker can tamper the node physically and manipulate the data. Cognizant information like the cryptographic keys can be extracted by the attacker. This may result in loss of important and further higher level of information. This attack occurs at physical layer of OSI. Temper proof physical packaging is one possible defensive strategy against such attacks.

### *3.3. Exhaustion (Continuous Channel Access)*

This attack occurs at the data link layer. The attacker interrupts and confuses the channel by iteratively asking queries and transmitting over it. It traps the channel and doesn't allow the legitimate users to access the channel and send the data packets. This often results in starvation. The sensor nodes are exhausted in terms of power as most of their energy goes wasted in serving the unwanted intrusive packets. One solution against this attack is limiting the request rate so that unnecessary requests can be discarded without wasting power. Yet the limit can't be set less than the conventional maximum data rate. Time division multiplexing can also be a probable solution for preventing such attacks as in this time slots are divided for every node.

### *3.4. Collision*

When any two nodes undergo concurrent transmissions over similar frequency channels collision can occur. When this happens, there is some change in the packet contents. This results in a mismatch when checksum is computed at the receiving end. As in case of mismatch the packets need to be re-transmitted so this leads to unnecessary energy consumption. Collision occurs at data link layer. To prevent such situation error correcting codes can be used at low collision levels.

### *3.5. Routing Information*

The prime focus of such an attack is on the routing protocols. The information contained in routing protocols can be changed. As the routing information changes, the packets follow a path different from the intended one and hence are misdirected. This attack occurs at the network layer.

### *3.6. Selective Forwarding*

For a reliable and secure communication, the information received at the destination must be exactly the same as sent by the source node. But the malicious nodes may selectively forward the packets to the subsequent node and drop the rest. This results in loss of important data. In case all the packets are dropped and none is forwarded, the attack is called blackhole attack. This attack affects the network layer. One of the solutions for this attack could be transmitting data through multiple paths. In this case if one path is affected by some malicious activity, another path may result in secure communication (Md Safiqul *et al*, 2011).

### *3.7. Sinkhole Attacks*

Network layer is affected by this attack. The surrounding nodes are forged by the attackers. The adversary attracts the nearby motes by using attractive bandwidth or path and fools the motes. The fooled motes route data to the compromised node resulting in packet dropping. This may further lead to selective forwarding or blackhole attack.

### *3.8. Sybil Attack*

The attacker in this case has multiple identities and fools the surrounding nodes. By taking the identity of other node it has access to the information meant for that node. Network layer is prone to such an attack. One countermeasure against Sybil attack is authentication and encryption (Padmavathi *et al*, 2009).

### *3.9. Wormhole*

In this attack, the attacker overhears the communication between two motes. It then replays information between the motes located far away physically by giving an illusion that they are very close to each other. This attack occurs at network layer.

### *3.10. Hello Flood Attack*

Hello packets are broadcasted to the network by the malicious nodes. High power RF transmitters are used.

This is done to make the nodes believe that the malicious nodes are the neighbourhood nodes. Thus the unauthorized users have the access to the channel. This results in loss of information as the legitimate user doesn't get the access to the channel. Network layer is affected by the hello packets.

### *3.11. Flooding*

Flooding attack occurs at transport layer. The adversary sends new connection request to the nodes again and again until the resources of the nodes are exhausted. The legitimate requests are thus ignored as the channel is occupied by the attacker.

### *3.12. Blackhole Attack*

In this attack the attacker take hold of the node and reprograms it. The attacker drops the packets and doesn't allow the node to pass the information to subsequent nodes. This results in complete loss of data packets (Ajit Pokharkar *et al*, 2015).

### *3.13. Denial-of-Service Attack*

A Denial-of-service (DOS) attack is an attempt to prohibit the genuine user of a service or data. The destination system is overwhelmed with fallacious requests such that it cannot acknowledge the genuine traffic. Thus the services are inaccessible to the authorized users. The efficiency of the system is affected; performance decreases and eventually the network stops functioning. Using the sensor networks in sensitive and critical areas intensifies the likelihood of DOS attacks. This attack drains off the energy of the node and knocks down the network (Krishna Doddapaneni *et al*, 2011).

### *3.14. Misdirection attack*

Misdirection attack is a kind of DOS attack. The incoming packets are misdirected to a mote other than the expected mote. This results in loss of important data. The intended user is deprived of the services; consequently leading to delay and decreased throughput (Muhammad Raisuddin *et al*, 2014). It can be performed in the following ways:

- Packets are delivered to mote close to the destination mote: This type of attack is less harmful and less powerful. The packets are routed to mote close to the intended one; they reach the destination following a different path and not the intended path. Thus the packets are delayed and the number of bits transferred per second i.e. throughput decreases.
- Packets are delivered to mote far away from the destination mote: this type of attack is more venomous. The packets are delivered to mote which is far away from the intended user and thus never reach the destination. This results in infinite delay and zero throughput (Sachan *et al*, 2013).

## 4. Countermeasures against the attacks

WSNs are prone to various types of attacks. Energy-efficient link layer jamming attack is one of the highly perceptible threats for these networks. In this the attacker drains away the energy of the nodes. There is unnecessary consumption of energy and large amounts of delay. The MAC protocol of the link layer is the main target of jammer. The Data Packet Separation Slot Size Randomization (DSSSR) and Round Robin (RR) slot size assignments are the modifications to the sub layer. These modifications aim at exhausting the energy of the jammer. The first modification divides the data packet into two parts and helps in bewildering the jammer by giving an illusion that the slot size is smaller in size. The jammer thus loses power by jamming at higher rate. The use of Round Robin eliminates adverse impact on throughput of network which would otherwise occur due to the first modification. The second modification ensures that all the nodes are able to transmit for equal time intervals (Ahmed R. *et al*, 2011).

Cluster based technique is an effective technique against the misdirection attack. This technique detects and isolates the malicious nodes from the network by forming clusters. Cluster head compares the parameters stored in its own buffer and the buffer of nodes through which data packets route and detects the malicious nodes. It then alerts the other nodes by passing the identity of the malicious nodes. The neighboring nodes thus block the malicious node (Sachan *et al*, 2013).

The wireless sensor network is usually static that is the nodes are not capable of moving. The attacker launches the attack by introducing mobile malicious nodes. Uncompromised nodes usually communicate at regular intervals of time but the mobile nodes after launching the attack at one location move to another location and stop communicating with the previous neighbourhood nodes. The nodes which are silent for longer time periods than expected are considered to be mobile in the otherwise static network. These nodes are thus blocked (Sajal K. Das *et al*, 2012).

The detection of malicious nodes is done without sacrificing fault free nodes in the presence of noise and natural faults. In a hierarchical sensor network Dual weighted trust evaluation (DWE) detects malicious nodes when the fault occurs. Two trust values are assigned to every sensor node. Trust values are the weights at each subsequent node. Fault free nodes have trust value close to one while the faulty nodes have a decrease in value which leads to their detection (Chan O. Hong *et al*, 2012).

Malicious nodes can be detected by using two thresholds instead of one. This technique is more efficient and gives better results than the one using single value of threshold.

**Table1** Different attacks in Wireless Sensor Networks

| Attack | Attack Definition | Effects of Attack | Countermeasures against Attack |
|---|---|---|---|
| Jamming | Malicious nodes hampers with the radio frequency used by the target | • Collision of packets during transmission<br>• Resource exhaustion<br>• Confusion | • Spread spectrum technique for radio communication<br>• Using algorithms which take into account Radio Signal Strength Indicator(RSSI) values, carrier sense time and Packet Delivery Ratio (PDR) techniques (Shahriar *et al*, 2011). |
| Tampering | Attacker tampers the node physically | • Damage the sensor node and hardware<br>• Extract sensitive information such as cryptographic keys and gain access to higher level information. (Shahriar *et al*, 2011). | • Using tamper-proof packaging |
| Collision | Two nodes simultaneously transmit traffic with same frequency | • Discarding packets<br>• Energy exhaustion<br>• Interference | • Error correction codes can be used but they require additional processing and communication overhead |
| Selective Forwarding | Malicious nodes are introduced in the network | • Packet dropping<br>• Loss of information | • Transmitting data through multiple paths |
| Sinkhole Attack | Attacker lures the target by means of attractive bandwidth and routing path | • Information alteration<br>• Packet dropping<br>• Exhaustion of resources<br>• Triggering of blackhole, wormhole and selective forwarding attacks<br>• Spoofing<br>• Replaying of old message ( Gaurav *et al*, 2013) | • Key management<br>• Authentication<br>• Geographic routing |
| Sybil Attack | The attacker masks multiple identities and fools the network | Threat to geographical routing protocols | • Outsider attacks can be prevented by authentication and encryption<br>• Inside attacks can be prevented by using public key cryptography but it is expensive (Gaurav *et al*, 2013) |
| Wormhole Attack (Gaurav *et al*, 2013) | Attacker overhears the message and tunnels to node located far away | • Change in network topology<br>• Triggering of blackhole, sinkhole and selective forwarding attacks<br>• Information alteration | • Authentication<br>• Link layer encryption |
| Hello Flood Attack | Hello packets are transmitted at high RF power to make the channel busy | • Data congestion | • Authentication of the two-way link before acting on the information<br>• Cryptographic and non-cryptographic techniques |

Compromised nods are detected with higher accuracy. False alarm rate decreases and event detection accuracy increases by using two threshold values. Malicious node detection rate increases without compromising the performance of fault –free nodes (Yoon-Hwa Choi *et al*, 2013).

LEACH is used for detecting grayhole attack, blackhole attack and misdirection attack. LEACH is an energy efficient protocol. Nodes are grouped into clusters based on the protocol. Cluster heads are made which handle the sensor nodes grouped in their cluster. The sensor nodes report the data to the cluster head. Using this protocol saves energy and prolongs the lifetime of the network (Yoon-Hwa Choi *et al*, 2012).

This method can be used against the denial-of-service attacks. Two lists are formed for distinguishing the fallacious packets and the legitimate data packets. On the basis of data contained in these lists the incoming packet is judged whether it is legitimate or malicious. The malicious node is thus identified using this strategy.

**Table 2** Techniques against the attacks

| S.No | Paper Title | Year | Author | Approach | Advantages | Disadvantages |
|---|---|---|---|---|---|---|
| 1. | Defending Against Energy Efficient Link Layer Jamming Denial of Service Attack in Wireless Sensor Networks (Ahmed R. *et al*, 2011). | 2011 | Mahmood, Ahmed R, Hussein H. Aly, and Mohamed N. El-Derini | Data Packet Separation Slot Size Randomization (DSSSR) and Round Robin (RR) slot size assignment modifications applied to the sub layer | Network throughput increases. Censorship rate decreases. Lifetime advantage of jammer decreases. | Wastage of time slot in case the node doesn't have data for transmission in the allotted slot. |
| 2. | Distributed detection of mobile malicious node attacks in wireless sensor networks(Jun-Won *et al*, 2012) | 2012 | Ho, Jun-Won, Matthew Wright, and Sajal K. Das | Sequential Probability Ratio Test (SPRT) is used. | The mobile malicious nodes in the static sensor network are detected. | Each time the network is redeployed which is very frequent due to removal of faulty nodes and addition of new sensor nodes, the neighbor discovery phase needs to be repeated. |
| 3. | Detection of HELLO flood Attack on LEACH Protocol (Magotra *et al*, 2014) | 2014 | Magotra, Shikha, and Kush Kumar | Non-cryptographic technique is proposed. Only those nodes which have RSS and distance within threshold limits are allowed to join CH. | Attack detection time, communication overhead, Energy consumed and computational power are reduced. Number of times the test packet is transmitted is reduced. | Malicious nodes are detected but are not isolated. |
| 4. | An improved Watchdog technique based on Power-aware Hierarchical design for IDS in Wireless Sensor Networks (Forootaninia *et al*, 2012) | 2012 | A. Forootaninia and M. B. Ghaznavi-Ghoushchi | CHs act as watchdogs and maintain a buffer consisting of the messages transferred among the nodes and use this buffer for malicious node detection | Problems of selecting incorrect malicious nodes, limited power transfer, node conspiracy and impartial removal are tackled effectively. | Creation of collisions in receiver and ambiguous collisions problems still prevail. |
| 5. | The detection and defence of DoS attack for wireless sensor network (Zhang *et al*, 2012) | 2012 | Zhang, Yi-ying, Xiang-zhen Li, and Yuan-an Liu | Two lists are created on the basis of which the incoming packet is judged whether it is malicious or not. Malicious node on being identified is blocked and cryptographic keys are used to rekey and reprogram the nodes. | Malicious nodes are detected with less energy consumption. Computational load is decreased. | Lacks the mechanism for reprogramming and rekeying. |

Malicious node ID is sent to the neighboring nodes which block that node. Thus the malicious node is no longer able to corrupt the data. Next the cryptographic keys are used to rekey and reprogram the nodes so as to protect them from further intrusion. This method reduces computation and lesser energy is consumed (Zhang *et al*, 2012).

HEED is an effective protocol in terms of energy consumption. Number of iterations required for satisfactory clustering is less and control overhead is also reduced. Residual energy in the node is used to decide the cluster head. The cluster heads report to the base station and session keys are distributed by Key Distribution System (KDS). This protocol is better than LEACH as the head of the cluster is decided on the basis of residual energy whereas in LEACH random selection of cluster head is done. It helps in increasing the network lifetime (Navaneethan *et al,* 2014).

## Conclusion

Although there are many strategies to act against the security attacks still an upgrade in the technology is needed. The attacks act against the security goals of the secure communication. They drain off the energy of the nodes and decrease the network lifetime. Measures need to be taken against the active and passive attackers in order to maintain the data integrity and authenticity. Security mechanism needs to be made more efficient. This could be done by making the protocols operating at different layers moreresistant to attacks. Cryptographic and clustering techniques could be used to strengthen the network against any kind of malicious activity. The above mentioned defensive techniques need to be made stronger so as to safeguard the network.

## References


Kaplantzis, Sophia, Alistair Shilton, Nallasamy Mani, and Y. Ahmet Şekercioğlu (2007), Detecting selective forwarding attacks in wireless sensor networks using support vector machines, *In Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on*, pp. 335-340. *IEEE.*

Ghildiyal, Sunil, Amit Kumar Mishra, Ashish Gupta, and Neha Garg, Analysis of Denial of Service (DoS) Attacks in Wireless Sensor Networks. *IJRET: International Journal of Research in Engineering and Technology* pp.2319-1163

Singh, Shio Kumar, M. P. Singh, and D. K. Singh. (2010), A survey of energy-efficient hierarchical cluster-based routing in wireless sensor networks, *International Journal of Advanced Networking and Application (IJANA) 2.02* : 570-580

Modares, Hero, Rosli Salleh, and Amirhossein Moravejosharieh (2011), Overview of security issues in wireless sensor networks, *In Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on,* pp. 308-311. IEE

Padmavathi, Dr G., and Mrs Shanmugapriya (2009), A survey of attacks, security mechanisms and challenges in wireless sensor networks." *arXiv preprint arXiv*:0909.057

Kavitha, C. (2012), A survey on secured routing protocols for wireless sensor network, *In 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12),* pp. 1-8

Agah, Afrand, and Sajal K. Das. (2007), Preventing DoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach. *IJ Network Security5, no. 2* pp. 145-153.

Lédeczi, Ákos, and Miklós Maróti (2012), Wireless sensor node localization. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 370,* no. 1958 pp. 85-99

Islam, Md Safiqul, and Syed Ashiqur Rahman (2011), Anomaly intrusion detection system in wireless sensor networks: security threats and existing approaches, *International Journal of Advanced Science and Technology 36,* no. 1 pp. 1-8 ,2011

Dhulkar, Ruchita, Ajit Pokharkar, and Mrs Rohini Pise (2015), Survey on different attacks in Wireless Sensor Networks and their prevention system

Ghosh, Arindam, and Krishna Doddapaneni (2011), Analysis of Denial-of-Service attacks on Wireless Sensor Networks using simulation. *IT Security for the Next Generation-European Cu*

Ahmed, Muhammad Raisuddin. (2014), Protecting Wireless Sensor Networks from Internal Attacks, *PhD diss., University of Canberra.*

Sachan, Roshan Singh, Mohammad Wazid, Dhirendra Pratap Singh, and R. H. Goudar (2013), A cluster based intrusion detection and prevention technique for misdirection attack inside WSN, *In Communications and Signal Processing (ICCSP), 2013 International Conference on,* pp. 795-801. *IEEE.*

Mohammadi, Shahriar, and Hossein Jadidoleslamy (2011), A comparison of link layer attacks on wireless sensor networks, *arXiv preprint arXiv:*1103.5589

Kulkarni, Gaurav, *et al*. (2013), Wireless sensor network security threats, *Communication and Computing (ARTCom 2013), Fifth International Conference on Advances in Recent Technologies in. IET*

Mahmood, Ahmed R., Hussein H. Aly, and Mohamed N. El-Derini (2011), Defending against energy efficient link layer jamming denial of service attack in wireless sensor networks, *In Computer Systems and Applications (AICCSA), 2011 9th IEEE/ACS International Conference on, pp. 38-45. IEEE*.

Ho, Jun-Won, Matthew Wright, and Sajal K. Das (2012), Distributed detection of mobile malicious node attacks in wireless sensor networks, *Ad Hoc Networks 10,* no. 3 pp. 512-523.

Oh, Seo Hyun, Chan O. Hong, and Yoon Hwa Choi (2012), A malicious and malfunctioning node detection scheme for wireless sensor networks. *Wireless Sensor Network 4,* no. 03 pp. 84.

Lim, Sung Yul, and Yoon-Hwa Choi (2013), Malicious node detection using a dual threshold in wireless sensor networks*, Journal of Sensor and Actuator Networks 2,* no. 1 pp. 70-8

Yim, Sung-Jib, and Yoon-Hwa Choi (2012), Neighbor-based malicious node detection in wireless sensor network

Zhang, Yi-ying, Xiang-zhen Li, and Yuan-an Liu (2012), The detection and defence of DoS attack for wireless sensor network, *The journal of china universities of posts and telecommunications 19* : pp. 52-56

Kumar, Dines. VS, Navaneethan. (2014), Protection Against Denial of Service (DoS) Attacks in Wireless Sensor Networks, *International Journal of Advanced Research in Computer Science & Technology (IJARCST 201*

Magotra, Shikha, and Kush Kumar (2014), Detection of HELLO flood attack on LEACH protocol, *Advance Computing Conference (IACC), 2014 IEEE International*

Forootaninia, A., and M. B. Ghaznavi-Ghoushchi (2012), An Improved Watchdog Technique based on Power-Aware Hierarchical Design for IDS in Wireless Sensor Networks. *arXiv preprint arXiv:1208.2079.*