WIRELESS SENSOR NETWORK SECURITY ISSUES: A BRIEF REVIEW

Padmalaya Nayak[1], M.Shanthi[2]

[1]*Professor, GRIET, Hyderabad*
[2]*Asst. Professor, GITAM University, Hyderabad*

Abstract

Wireless Sensor Network (WSN) applications are growing tremendously in many areas that ranges from environmental and habitant monitoring to health care, agriculture, military, defense, control and tracking applications. Despite of huge growth in applications, these networks are prone to security attacks. Again, deployment of these networks in a hostile and unattended environment along with the limited resources make the design/deployment issue more critical than any other networks. Recently, many research publications discuss on the security issues and challenge involved in WSN why because the limited source of nodes can't provide a desired level of security by itself. Even though many studies discuss many potential issues of WSN security, most of these are discussed in isolation of each other. Keeping this in mind, trying to provide a clear picture of this vast area, attempt has been made to present the major security issues that consider the probable attacks and how it can be detected prior to the attack and various detection mechanisms are discussed in this paper. A brief taxonomy of WSN constraints and different types of attacks and detection mechanisms are presented this paper.

Keywords—*WSN, WSN Attacks, IDS*

----------***----------

1. INTRODUCTION

A Wireless Sensor Network consists of huge number of tiny sensor nodes deployed in a harsh environment and work collaboratively to achieve a common phenomenon. These sensor nodes have limited resources such as energy, memory, processing and computational capacity. The first sensor network application was Sound Surveillance System (SOSUS) in early 1950 [1]. SOSUS is still in active for monitoring seismic and animal activity in the ocean [2]. Later around 1980s, Defense Advanced Research Project Agencies (DARPA) initiated distributed sensor projects (DSP). Recent advancements in VLSI design and wireless communication led to the development of small and low cost processors permits for huge WSN applications. WSN is susceptible to many types of attacks at each layer of TCP/IP suite and traditional security mechanisms [14] are not suitable for it. There are various reasons for it. Un-trusted transmission, open environment deployments, unattended operation, and limited resources make the WSN more unsecure. Further inherent nature of wireless communication makes the network more vulnerable. Sensor Networks employ battery recharging policy which is very difficult task and may not even possible as the nodes are deployed in a hostile environment. For any type of application, the design goal of WSN is to keep the sensor network alive for longer period of time by consuming less amount of energy [5]. Among all the design aspects of WSNs, security is the main important aspect that deserves great attention considering tremendous application opportunity. There are many categories of attackers and they can destroy or damage the network partially or completely. Few of them have been focused below.

- **Passerby**
  These types of attackers are not determined and motivated spontaneously. They have little knowledge about the network and require few resources

- **Vandal**
  These types of attackers have little knowledge and desire to cause damage. They are determined moderately and require few resources to achieve the target.

- **Hacker**
  Hackers are highly knowledgeable and motivated by their own curiosity and interest. They are determined to cause damage and require moderate resources.

- **Raider**
  Raiders are mostly interested in political gain. They are also highly determined and knowledgeable personnel. They require moderate resources to achieve organization/personal monetary gain.

- **Terrorist**
  Terrorists are belongs to high class category of attackers and strongly determined, highly knowledgeable and intended to cause real world damage. Mostly, they are motivated by enmity and they are very powerful with respect to time, power and money.

The above all categories of attackers can manipulate the network, disrupt the network and finally they can destroy the network. The various categories of attackers that intend to destroy the network are shown in Fig.1. The major

contribution of this paper is to lead the researcher towards the current security issues for WSN and provide some open research problem to be handled by the interested researchers.

The reminder of the paper is organized as follows. Section II discusses about the security related issues such as security goals, WSN constraints, security threats, and security mechanisms. Section III discusses about major types of attacks in WSNs. Section IV presents on the denial of Service (DoS) attacks and countermeasures for it. Section V gives an overview of detection mechanisms available in the current literature followed by a concluding remark.

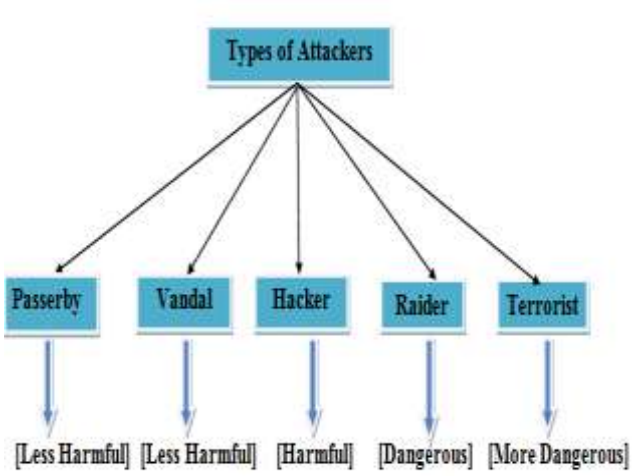

Fig 1: Types of Attackers

Table 1: Characteristics of different types of Attacker

	Types of Attacker				
Characteristics	Passerby	Vandal	Hacker	Raider	Terrorist
Motivation	Spontaneously	Own interest to cause damage	Own curiosity and interest	Political gain	By enmity
Determination	Nil	Moderately	Highly	Highly	Strongly
Resource Requirement	Few	Few	Moderate	Moderate	More
Knowledge Requirement	Little	Little	High	High	High

2. SECURITY CONCERNS IN WSN

The main aspects of Wireless Sensor Network Security can be classified into four major categories; Security goals, WSN Constraints, Major types of attacks and detection mechanisms.

2.1 Security Goals

Wireless Sensor Network is considered as a special category of ad hoc networks. The security goals of WSN can be divided into two major categories such as standard goal of traditional network and unique goal of ad hoc sensor networks. The standard goal incorporates data confidentiality, data authentication, data integrity, data availability, data freshness and the unique goal incorporates self organization, time synchronization, secure deployment, wide application, cost effective, privacy and autonomy etc.

2.1.1 Standard Goal

- **Data Confidentiality**
  Data confidentiality is the first and most important security issues that need to be considered for any type of networks. Particularly, the sensor node carrying the data should not be modified or passed to the neighbor nodes for any type of applications. Most of the time, the sensor nodes carry highly sensitive data. So, it is extremely important to provide a secure channel for WSN.

- **Data Authentication**
  Authentication is another important and crucial goal for many WSN applications. An adversary not only tries to modify the contents of the data packet but also change the whole content by injecting the additional data packets. So, data authentication claims that any receiver has been received the data that has been sent by the original sender. To achieve this, the sender and receiver share a symmetric shared secrete key to compute the message authentication code (MAC) of all transmitted data.

- **Data Integrity**
  Data Integrity is a major issue to be considered. By implementing confidentiality, any adversary may not be able to still the data, but can add the malicious data packet that creates misconception that the received data by the receiver as the original data. Even if in the absence of adversary, data can be lost or corrupted as the senor networks are deployed in an uncontrolled environment. Data Integrity ensures the reliability of the data and it should not be altered or tampered during the transmission.

- **Data Freshness**
  Data freshness ensures that the data received by the receiver is recent data and no old message is replayed. It mostly happens when shared keys are employed in the design. So, shared keys must be changed over time. Normally, the new keys take time to propagate throughout the network. At that point the adversary gets an opportunity for replay attack. To avoid this problem, a nonce or time related counter is added in the packet to ensure data freshness.

- **Data Availability**
  The sensor network must be capable enough to provide the services at the time of the user's need. So, the hardware and software components must be robust enough to provide services even if in the presence of malicious entities or adverse situations. This property requires itself a security mechanism. All protection mechanisms must be energy efficient so that the batteries of each node should not be drained quickly.

2.1.2 Unique Goals

- **Self Organization**
  WSN is belongs to the category of ad hoc networks that does not require any infrastructure to be established. Each node is independent with self organizing capability to communicate with each other in different types of environments. The inherent nature of sensor node makes the sensor network security challenging.

- **Time Synchronization**
  Time synchronization is an important factor for sensor network that is responsible for maintaining the consistency of the network. Specifically, for tracking application, sensor network requires group synchronization [11] to know the exact sequence in which events such as alarm occurred. All the nodes must be equipped with similar clocks to maintain the time synchronization regardless of the hardware problems such as offset, skew, and drift problem. Many synchronization protocols must know the timing information of both the sender and receiver. Moreover, time synchronization is needed to ensure a secure communication channel in order to avoid attack.

- **Secure Deployments**
  Whenever a large number of sensor nodes are required to deploy in a hazardous or remote environments, deployment issue is a big challenge to be handled. If the sensor network is employed in a known place, the exact position of the node can be known. But if the senor network is deployed in a remote jungle, nodes can be deployed from the airplane. So, there is no certainty about the positioning of the sensor nodes. A localization algorithm is used to compute all the positions.

- **Wide Application**
  As discussed above, WSN application domain varies widely, security threats also vary exponentially because the threats are application specific. So, there are no single mechanisms that can provide tightened security for all type of sensor networks by compromising the cost. For instance, battle field applications are more prone to DoS attack whereas habitat monitoring or other environmental attacks are subject to eavesdropping or stealthy attacks.

- **Privacy and Autonomy**
  It is another security related issue that is beyond the technological dimensions and affects its social environment. The location and identity of base station and other sensor nodes that are generating the information must be hidden and protected. It is extremely important in case of battle field where one should not distinguish certain signals belongs to the solider or a vehicle. But this property must not be enforced in case of earth quake. In that situation, the source node must be absolutely located.

2.2 WSN Constraints

2.2.1 Node Constraints

- **Limited Memory and Storage**
  Each sensor node is a very small device having little amount of memory and storage space for coding in order to ensure effective security algorithms. For example, one common type of senor (TelsoB) has 16 bits, 8 MHz RISC CPU with 10K RAM, 48K program memory, and 1024 flash storage [3]. With this limitation the software built must be quite small. The total code space for tinyOS, the de-facto standard for wireless sensors is approximately 4K and core scheduler occupies 178 bytes only [4]. Due to this reason, the security algorithms must be small enough to fit with the small storage.

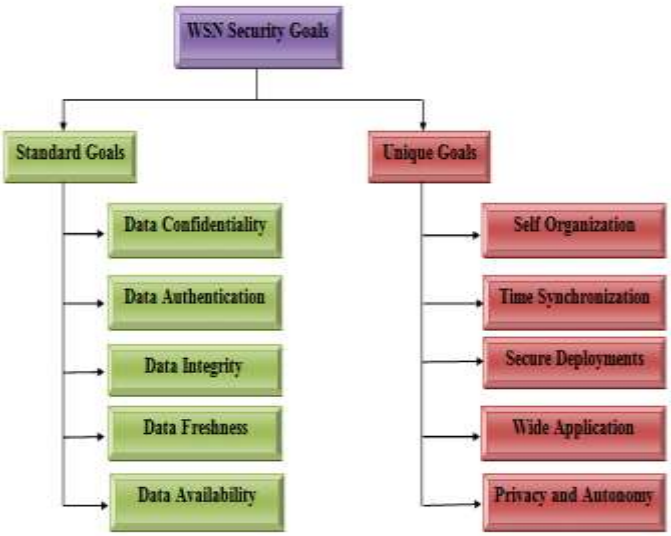

Fig 2: WSN Security Goals

- **Energy Constraints**
  Energy consumption in WSN at node level can be categorized into three parts:
  –Energy for the sensor transducer
  –Energy for communication among sensor nodes
  - Energy for microprocessor computation

It is discussed in [17, 18] that each bit transmitted in WSNs consumes about as much power as executing 800–1000 Instructions. Thus, communication is more costly than computation in WSNs. Any message extension caused by security mechanisms comes at a significant cost. Further, sensor nodes are deployed in a harsh environment where human attendant is not possible. Once the sensor nodes are

deployed, battery recharging or replacement is out of question. So, the battery charge of individual network must be conserved so that the entire network can survive as for long time.

2.2.2 Network Constraints

- **Unreliable Communication**
  Wireless communication by nature itself is prone to error. It is another threat to the sensor network security. All most all the security mechanisms rely on the protocol and algorithm which in turn depends on the communication.

- **Ad hoc and Wireless Communication**
  Typically, sensor nodes are deployed randomly in the area of interest to monitor a common phenomenon where links are fragile and mostly asymmetric. The self-organizing property makes them to communicate with each other and to reach at the base station. This ad hoc radio communication makes the sensor network more challenging.

- **Lack of Infrastructure**
  A Sensor Network operates in a distributed manner without a central coordinator. This makes each node more vital for wireless communication. As no central point is there to co-ordinate and if the network is not well designed, it will make the organization difficult, inefficient, and fragile.

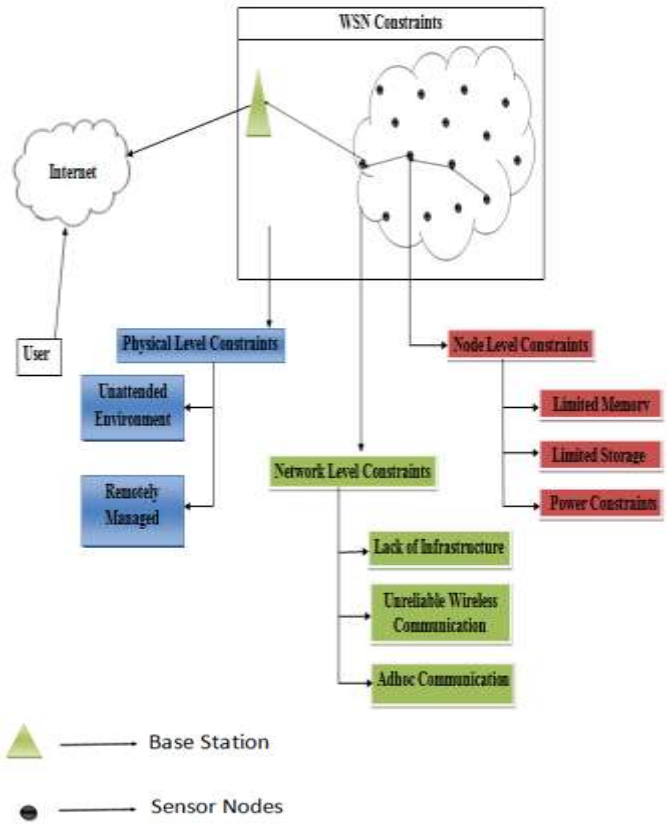

Fig 3: WSN Constraints

2.2.3 Physical Constraints

- **Unattended Environment**
  Normally, Sensor networks are deployed in an open environment, where these nodes are exposed to bad weather, adversaries etc. In such cases these nodes can not be attended by human and suffers with physical attack whereas normal PCs are placed in a secure place and get attack from the network only.

- **Remotely Managed**
  Typically WSNs are managed from remotely and it is nearly impossible to detect physical tampering and physical management issues such as battery recharge and replacement.

2.3 Security Threats

- Threat against Authentication and Confidentiality [16]: Cryptographic techniques are used to protect this type of attack.
- Threat on Availability [16]: Mostly it is known as Denial of Service attack. It targets each layer of the protocol stack. There is no clear single protection mechanism for this type of attack.
- Threat on Integrity [16]: It is known as stealthy attack. By this attack, it makes the network fool by accepting false data streams by compromising the nodes and injects false data through it.

2.4 Security Mechanisms

The major attraction of security mechanism is to detect, prevent, and recover from the security attacks. To provide a secure environment for WSN, different types of mechanisms are adopted. It can be provided in a lower level or higher level. The different types of security mechanisms are discussed below.

Low Level

At the lower level, the security mechanisms are provided by setting-up cryptographic keys among the sensor nodes and aggregating nodes. Again, the cryptographic keys must be scalable for huge no. of sensor nodes. In particular, the public key cryptography is too expensive to follow the small sensor nodes as the communication pattern of WSN is different from any other network. But, the drawback in this approach is that some compromised nodes can break up the keys completely.

High Level

Higher level security mechanisms include secure group management, secure data aggregation, and intrusion detection techniques. As sensor nodes work in a group, secure protocols for group management and data aggregation must be used. Again, WSNs are susceptible to many types of attacks. So, strong detection mechanisms have been developed to detect the intrusion [17].

3. MAJOR TYPES OF ATTACKS IN WSN

Sensor networks are vulnerable to different types of attacks due to the inherent nature of the common communication channel. Additionally, WSNs tend to be more vulnerable due to the ad hoc deployment of sensor nodes in a dangerous environment where the nodes are not protected physically. Basically, WSN attacks are divided into three major categories [16]. These are passive vs. active attacks, outsider vs. insider attacks, and laptop vs. mote class attacks. Fig. 1 depicts the classification of Wireless Sensor Network attacks in detail.

3.1 Passive vs. Active Attacks

Passive Attacks

The monitoring and listening to the communication medium without the knowledge of the sender and receiver is known as passive attacks. These are monitoring and eavesdropping, traffic analysis, and camouflage adversaries.

Monitoring and Eves Dropping

This is the most common attack that disturbs the privacy. By closely monitoring and overhearing the communication channel, the adversary can collect enough data and discloses it.

Traffic Analysis

Even if the messages are encrypted during transmission, still it is possible to analyze the traffic pattern. By observing the sensor activities, the adversary can cause the damage to the sensor nodes.

Camouflage Adversaries

The adversaries insert their nodes secretly inside the sensor networks and these nodes behave as the normal nodes to attract the packets. Once they receive the packets, they misroute the packets after analyzing the private information.

Active Attacks

Denial of Service

The main intension of the Denial of Service (DoS) attack is not only to subvert, disturb, and destroy the network but also to diminish or eliminate the service capability of the networks. Different types of DoS attacks could be performed at different layers of WSN. For instance, black hole and gray hole attack is an example of DoS attack at network layer of TCP/IP stack.

Physical Attacks

Unlike other attacks, physical attack is more sensitive to WSNs and destroys the sensor nodes permanently. As WSNs are deployed in an open environment without the human attention, it makes them highly susceptible for the physical attacks. An adversary tries all possible combination of the cryptographic keys, tamper it and modify the programming in the sensors or replace with the malicious sensors under the control of the adversary. In [10], it is referred that even if standard sensor nodes such as MICA2 Mote can be compromised within 2 seconds.

Message Corruption

If any content of the message is modified by an attacker, it does not maintain its integrity.

False Node

In WSN, many times malicious nodes are injected into the network secretly. It is one of the most dangerous attacks as the malicious node feeds false data to the network and blocks the original data. Once the malicious codes are injected in a network, it could spread all over the network, potentially destroy the whole network and finally, adversary takes the full control over the network.

Node Replication Attack

In this type of attack, an adversary adds extra node to the sensor network by copying the ID of an existing sensor nodes. Packets can be corrupted or misrouted resulting a disconnected network. If the adversary obtains physical access to the network, he can copy the cryptographic keys in the duplicated sensor nodes. So, he can manage a specific segment of a network.

Routing Attacks

Many types of routing attacks occur at the network layer. Some of the few known routing attacks are discussed below.

1. ***Wormhole attack***
   Wormhole attack is the most dangerous attack in WSN routing. In wormhole attack, two or more malicious nodes collaborate with each other to set up a channel with lower latency through which they can forward the packet and replay the packet locally.
2. ***Black hole Attack***
   In black hole attack, the injected malicious node drops all the packets instead of forwarding the packets to neighbor nodes.
3. **Sink hole Attack**
   In sink hole attack, the malicious node drops and forwards the packet selectively to the neighbor node. The adversary makes its own pattern to drop or forward the packets. It is also known as gray hole attack.

3.2 Outsider vs. Insider Attack

The distinction between outsider and insider attack is based on the knowledge and scopes of the adversary. As the name implies, an outside adversary attack from outside of the network boundary and uses his own devices to perform the attack. It has no privilege to access the data storage at sensor nodes of the WSN. An insider adversary can access the data stored at each node and uses this data to perform subsequent attacks. This insider attack can be lunched from any compromised nodes running malicious codes or by any laptops stealing the cryptographic key or data from the legitimate nodes.

3.3 Mote Class vs. Lap top Class attack

In mote class and lap top attack, adversaries can be distinguished based on the resource capabilities. A mote class adversary tries to gain access the sensor nodes with the similar capabilities like the sensor nodes deployed in the network. But, a laptop class adversary may gain access to more powerful devices like laptops with more resources such as more battery power, more powerful CPU, large memory space, a high power transmitter or a sensitive antenna.

4. MAJOR TYPES OF IDS MECHANISMS

In WSN, authentication and data encryption are not enough for ensuring data security. Another mechanism to protect SNs involves mechanisms for detecting and reacting to intrusions. An Intrusion Detection System (IDS) [21-24] monitors a host or network for suspicious activity patterns outside normal and expected behaviour.

- **Anomaly based IDS**
  In Anomaly based IDS system [23], identification of Intrusion can be achieved by analyzing the history of the test signal which is called unsupervised data or by collecting the training data which is called semi supervised data. The data set can be discrete, continues, or multivariable.
- **Signature based IDS**
  The signature based IDS system is also known as rule based IDS systems [15]. These IDS have pre-defined rules for different security attacks. Any deviation of the network behavior from the pre-defined rules is classified as an attack. One major advantage of these types of techniques is low false positive rate.
- **Specification based IDS**
  Specification based system is a form of anomaly based detection system with slight deviation. It looks for any abnormal behavior at the system level. These types of IDS define a legitimate behavior and when the system departs from this model, it can detect an intrusion.
- **Hybrid based IDS**
  This is the combination of anomaly based and signature based IDS system. It inherits the basic properties from anomaly based as well as signature based IDS system. One detection module verifies the known attacks using signatures and other module monitors the overall network behavior deviation from normal behavior. It is the most accurate detection system with less number of false positive. The major drawback of the hybrid system is it requires more energy and resources.
- **Cross layer IDS**
  Cross layer IDS can be applied at any layer of TCP/IP protocol stack. It uses cross layer interface to detect intrusion at each layer of TCP/IP stack by monitoring, communicating and exchanging the information. The main drawbacks of this type of IDS it is expensive in terms of cross layer interface.

Fig 4: Types of Attacks in WSN

5. CONCLUSION

The huge applications of Wireless Sensor Network ranges from environmental monitoring to military, defense, health care, agriculture etc. brings many more challenges to be analyzed. Among all the design issues, security is a major concern to be investigated. It is expected that Wireless Sensor Network would play a major role in future Internet of Things (IoTs) for monitoring, sensing, and identifying the objects uniquely through internet service. In this Paper, a detail summary of Wireless Sensor Network security issues has been provided hoping that it will provide a basic platform to carry out the further research work for the interested researchers. When these tiny sensor nodes would obtain the Internet connectivity to identify each object in this world, security must be provided at node level, network level and remote server level etc. So, some of the major threats has been discussed in this paper. Assuming that the encryption and authentication mechanisms cannot provide the desired level of security, some detection mechanisms have been discussed in this paper.

REFERENCES

[1] J. Pike, "Sound Surveillance System (SOSUS)," [Online] available at http://www.globalsecurity .org/intell/systems/sosus.htm, November 2002.

[2] Chee-Yee Chong, and S.P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges," Proceedings of the IEEE , Vol. 91, No.8, August 2003.

[3] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. E. Culler, and K. Pister. System architecture directions for networked sensors. In *Architectural Support for Programming Languages and Operating Systems*, pages 93–104, 2000. Hints: http://www.xbow.com/wireless home.aspx, 2006.

[4] D. W. Carman, P. S. Krus, and B. J. Matt., "Constraints and approaches

[5] for distributed sensor network security." Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, 2000.

[6] Y.Xu, J.Heideemann, and D.Estrin, "Energy conservation by adaptive clustering for ad-hoc networks," in *Poster session of MobiHoc'02*, 2002.
[7] R. Watro *et al.*, "TinyPK: Securing Sensor Networks with Public Key Technology," *SASN '04: Proc. 2nd ACM Wksp. Security of Ad Hoc and Sensor Networks*, New York: ACM Press, 2004, pp. 59–64.
[8] Y.-C. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," *IEEE Security & Privacy Special Issue: Making Wireless Work*, vol. 2, no. 3, May/June 2004, pp. 28–39.
[9] R. Roman, J. Zhou, and J. Lopez, "Applying intrusion detection systems to wireless sensor networks," in Proceedings of the 3rd IEEE Consumer Communications and Networking Conference (CCNC '06), pp. 640–644, January 2006.
[10] Zhang Y Y, Park M S, Chao H C, et al. Outlier detection and countermeasure for hierarchical wireless sensor networks. IET Information security, 2010: 361-373
[11] Zhou Y. Securing wireless sensor networks: a survey. IEEE Communications Surveys & Tutorials, 2008: 6−28
[12] Han G J, Shen W, Trung Q D, et al. A proposed security scheme against
[13] denial of service attacks in cluster-based wireless sensor networks. Security and Communication Networks, 2011
[14] Nanda R, Krishna P V. Mitigating denial of service attacks in hierarchical wireless sensor networks. Network Security, 2011: 14-18
[15] Raymond D R, Midkiff S F. Denial-of-service in wireless sensor networks:attacks and defenses. IEEE Pervasive Computing, 2008, 7(1): 74−81
[16] Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, Wireless sensor networks: A survey. Comput. Netw., 2002, 38: 393-422. DOI: 10.1016/S1389-1286(01)00302-4.
[17] Silva, A.P.R.D., M.H.T. Martins, B.P.S. Rocha, A.A.F. Loureiro and L.B. Ruiz *et al.*, "Decentralized intrusion detection in wireless sensor networks. Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks" , 2005, (QSSWMN; 25), pp: 16-23. DOI: 10.1145/1089761.1089765
[18] Shi, E. and A. Perrig, 2006. Designing secure sensor networks. IEEE Wireless Commun., 11: 38-43. DOI: 10.1109/MWC.2004.1368895
[19] J. Hill et al., "System Architecture Directions for Networked Sensors," ASPLOSIX: Proc. 9th Int'l. Conf. Architectural Support for Programming Languages and Operating Systems, New York: ACM Press, 2000, pp. 93–104.
[20] J. Hill *et al.*, "System Architecture Directions for Networked Sensors," *SIGOPS Oper. Syst. Rev.*, vol. 34, no. 5, 2000, pp. 93–104.
[21] A.D. Wood and J.A. Stsnkovic, "Denial of Service in Sensor Networks" Computer, Vol. No. 35, No. 10, pp. 54-62, 2002.
[22] David R. Raymond, Scott. F. Midkiff "Denial of Service in WSN: Attacks and defences, "IEEE pervasive computing, Vol. 1, No. 7, pp. 74-81, 2008.
[23] S. Marti *et al.*, "Mitigating Routing Misbehavior Mobile Ad Hoc Networks," *MobiCom '00: Proc. 6th Annual Int'l. Conf. Mobile Comp. and Net.*, New York: ACM Press, 2000, pp. 255–65.
[24] [Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," *Wireless Networks*, vol. 9, no. 5, 2003, pp. 545–56.
[25] Y. Huang *et al.*, "Cross-Feature Analysis For detecting Ad-Hoc Routing Anomalies," *ICDCS '03: Proc. 23rd Int'l. Conf.Distributed Computing Systems*, Providence, RI, May 2003.
[26] Y. Huang and W. Lee, "Attack Analysis and Detection for Ad Hoc Routing Protocols," *RAIS '04: Proc. 7th Int'l. Symp. Recent Advances Intrusion Detection*, Sophia Antipolis, France, Sept. 2004
[27] Xu., W. Trappe, W. Zhang., et.al., "The feasibility of Launching and detecting Jamming attachs in Wireless Networks" ACM MobiHoc'05, May 25-27, 2005, Urbana-Champaign, Iiiinois, USA, PP 46-57.
[28] A. P. R. Da Silva, A. A. F. Loureiro, M. H. T. Martins, L. B. Ruiz, B. P. S. Rocha, and H. C.Wong, "Decentralized intrusion detection in wireless sensor networks," in Proceedings of the 1st ACMInternationalWorkshop on Quality of Service and Security in Wireless and Mobile Networks (Q2SWinet '05), pp. 16–23, Montreal, Canada, October 2005.
[29] S. Banerjee, C. Grosan, and A. Abraha, "IDEAS: Intrusion detection based on optional ants for sensors," in Proceedings of the 5th International Conference on Intelligent Systems Design and Applications (ISDA '05), pp. 344–349, September 2005.