STUDY OF VARIOUS ATTACKS ON WIRELESS SENSOR NETWORKS

RAKESH SHARMA
Assistant Professor, Department of Computer Science,
CRM Jat College, Hisar

ABSTRACT: *Wireless sensor network (WSN) is a technology that emerges as result of various technologies. Initially, WSN have applications in defense and disaster management purpose but the accessibility of industrial, scientific and medical organizations extends its application area to public applications domain. WSNs own different characteristics such as self-organization and configurable, limited power, memory and bandwidth for communication, significant quantity of nodes, wireless, and infrastructure-less and many more. Hence, when setting a WSN, these characteristics must be considered so that a reliable and secure network is established. Various security schemes are employed to secure the WSN but these schemes provide first line of defense. To detect various attacks and malicious behavior, IDS proved to be an efficient solution. It is immensely difficult to recognize malicious behavior by employing traditional IDS in WSNs due to the distributed nature of DoS and black hole attacks. Considering the nature and characteristics of WSN, explicit IDS are needed for WSN.*

1. INTRODUCTION

Wireless sensor network (WSN) is a technology that emerges as result of advancement in various technologies such as wireless communication that includes IEEE (Crow brain, Widjaja, Kim Geun, and Sakai, 1997), Bluetooth (Bisdikian, 2001), Mobile Adhoc Networks (MANETs) (Corson and Macker, 1999) etc. and Micro-Electro-Mechanical Systems (MEMS). A WSN is defined from Smart Dust program of Defense Advanced Research Project Agencies (DARPA) as: "A sensor network is a deployment of massive numbers of small, inexpensive, self-powered devices that can sense, compute, and communicate with other devices for the purpose of gathering local information to make global decisions about a physical environment" (Olariu, 2005).Initially WSN have applications in defense and disaster management purpose, due to the accessibility of industrial, scientific and medical (ISM) band (2.4 GHz) also extends the application area of WSN to public applications domain. A massive amount of small sensor nodes that can reach out with other nodes using wireless mediums create WSN. Theses sensor nodes have restrictedcomputing and sensing capabilities. WSNs own different characteristics such as self-organization and configurable, limited power, memory and bandwidth for communication, significant quantity of nodes, wireless, infrastructure-less, and many more. Hence, when setting a WSN, these characteristics must be considered so that a reliable and secure network is established. However, the sensor nodes are equipped with sensing device known as sensor, computation processor for data processing and radio transceiver for communication with each other. Basically WSNs are depends upon the collective attempt of widespread sensor nodes, and these sensornodes are position densely all over the application range where they observe precise and accurate information. These sensor nodes communicate with everyone or with more than one sink nodes and these nodes cooperate with each other and along an isolated client. That can introduce query into the WSN by means of the sink nodes to carry out various operations such as distribution and gathering of information, processing of information and transmission of information operations to the sensors that sensed data from the network.

1.1. DESIGN OF WSN

In comparison to mobile ad-hoc networks, WSNs are resource restricted and large numbers of nodes are massively arranged. WSN geography is dynamic and thus prone to failures. Broadcast communication mediums are used for communication and at last sensor nodes don't have universal discovery identification (Karp, and Kung, 2000). Considering these factors sensor field, sensor node, sink, and task manager are the main segment of a WSN.
Source: Internet.

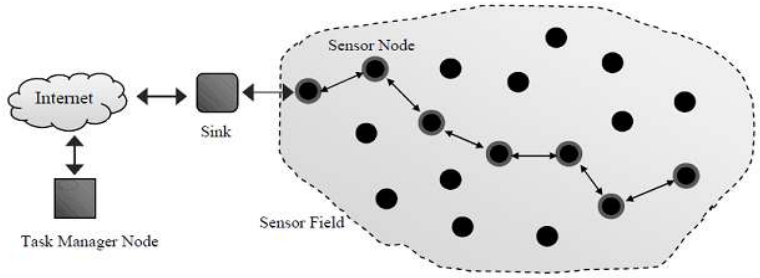


Fig.1.1 Layout of WSN

Sensor Field: It is a space in which sensor nodes are positioned for sensing.
Sensor Nodes: Sensor nodes are the main components of any WSN that are responsible for the working of the sensor network. Their main function is collection and routing of sensed data.
Sink: It is a special dedicated node whose work is to receive process and store the data coming from the other sensor nodes. Their main motive is to compile the messages that must be transmitted, and thus reduce the energy usage of the WSN. And sink nodes are dynamically positioned into the network. Regular nodes can act as sink node if they send aggregated outgoing messages. Therefore sink nodes are in addition designate as data aggregation nodes.
Task Manager: The centralized spot of self-control that is admitted as base station is act as the task manager of the WSN whose work is to broadcast controldata in the system and mine information from the system. Other major function of task manager is that it acts as a gateway to dissimilar systems. It is a dedicated storage point and data processing and an interface to the remote user. A laptop or a workstation can be act as task manager. Information is flooded to these task managers either via the wireless channels, satellite, and internet.

1.2. ISSUES RELATED TO WSN

As the application area for WSN is increasing day by day. WSN gives solutions to many real day to day problems whether it is agriculture, environment or industry it is applicable to all. As the technology is improving day by day, different types of sensor nodes such as multi-purpose nodes (generic node) and bridge nodes (gateway node) are available in the market. A multi-purpose node's can be utilized to collect aggregate data from the sensed location. It can be combination of different devices so that it can sense different physical properties such as velocity, magnetic field, temperature, acceleration, barometric pressure etc. whereas bridge nodes are the special nodes whose function is to gather information from the multi-purpose nodes and communicate to the base station. Capabilities of bridge node are more than the multipurpose nodes in stipulations of battery potential, transmission (radio) range, and processing capability. WSN is set up usually with the combination of both nodes. To take full advantage of remote sensor system, the scale of work can be broadly arranged into three configurations as appeared in Fig. 1.2. Primary configuration is the framework of the WSN. Every sensor node in the WSN is an individual framework. To deploy a WSN, different application software is needed to sustain on a WSN, new platforms, operating systems (OS) and memory is required. Secondary configuration includes communication protocols and administration. Communication protocols, which are responsible for carry out interaction between node and application.
Administrations are required to carry out the various administrative functions such as upgrade the operation and to promote WSN efficiency and performance. Because of function necessities and considering the board points of view, the sensor nodes are robust for self-arranging themselves and therefore can control and manage themselves proficiently. The communication protocol model is similar to standard TCP/IP model. Pursuit of protocols at various tiers in the procedure stacks can in general control power utilization, rescheduling, and framework productivity. And it is critical to improve transmission and limit power use. As they work on restricted characteristics of the WSN such as power consumption, etc. due to continuously working of sensor system, the node is drained out of power, i.e. die and detach from the system that reduces the performance of the application.
Source: Yick, Mukherjee, and Ghosal, (2008).

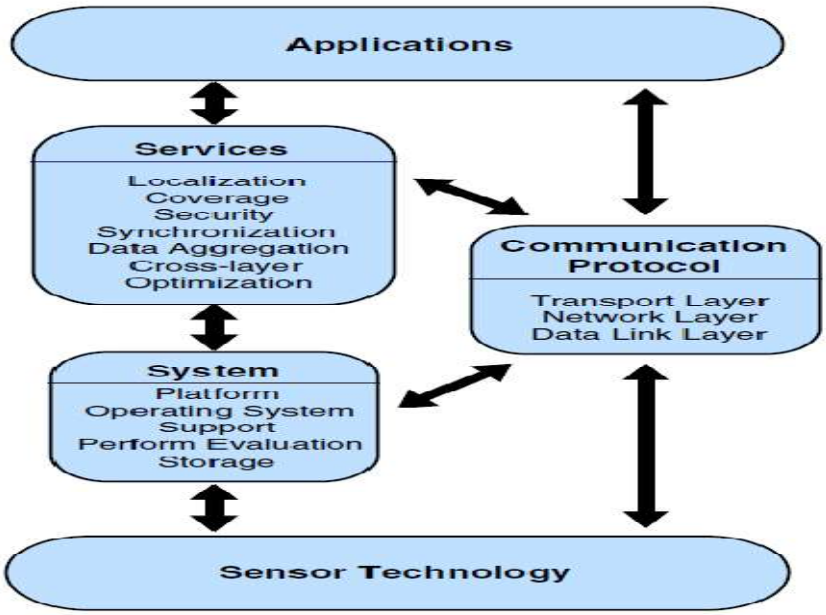


Fig. 1.2 Framework of WSN

WSN lifetime relies upon the quantity of dynamic nodes and availability of the system, so power must be utilized effectively so as to enhance the network lifetime. Nodes gather power from an power source. Potential power origin incorporate sunlight based cells (Raghunathan, Kansai, Hse, Friedman, and Srivastava, 2005), (Zhang, Sadler, Lyon and Martonosi, 2004) vibration (Roundy, Rabaey, and Wright, 2004), power modules, acoustic commotion, and a multipurpose source (Rahimi, Shah, Sukhateme, Heideman, and Estrin, 2003). To gather energy from the environment (Kansai and Srivastava, 2003), solar system is the best technology for energy gathering. Efficient power preservation in a WSN in turns expands the network lifetime. And power conservation can be achieve through use of efficient reliable wireless communication, proper placement of sensor nodes, efficient storage management, security, efficient data aggregation and compression. A advanced scale of analysis could be essential to enlarge the precision of the sensed data depending on the application.

1.3. SECURITY IN WSN

The applications of WSN in various fields are increasing day by day and the technology is also improving dynamically. Therefore, security concerns in these systems are also increasing. There are numerous strategies that make WSN indifferent. New methods are constantly emerging to attack WSNs. (Mohammadi, Ebrahimi, and Jadidoleslamy, 2011), (Guorui, Jingsha, and Yingfang, 2008). To prevent WSNs from various risks and different types of attacks, vulnerabilities present in the WSN should be addressed (Wazid, and Das, 2016), (Yick, Mukherjee, and Ghosal, 2008). For the need of system quality, fault tolerant, information precision, classified and delicate functions of WSNs, as protection is a crucial prerequisite in these systems and it ought to build up as indicated by their requirements to take care of security issues and shortcomings of these systems. The security of WSN is focused on integrity and availability of the system, authentication and authorization of source, and integrity and confidentiality of data. In this manner, security in WSNs is a vital, basic issue, and necessity. Securing WSNs is a very vital concern; particularly when the applications considered for WSN whose nodes are deployed in hostile environments. WSN security faces many challenges that may possibly not come across in other wireless systems.

1.3.1. SECURITY GOALS FOR WSN

WSN basically has two types of security goals such as primary and secondary. Primary goals are confidentiality, integrity, authentication and availability. They are also recognized as CIA standard protection goals. Secondary goals are Time Synchronization, Data Freshness, Secure Localization, and Self Organizations are secondary.

- Data Confidentiality: It is the fundamental security issues in WSN that ensures that the message passing through different nodes remains confidential. Confidentiality is the ability to secure sensor node so that data cannot be expose to it's the neighboring nodes.
- Data Authentication: The reliability of the message from its place of beginning is ensures by data authentication.
- Data Integrity: Data integrity will be accomplished in nature as a harmful sensor node present in the system can compromised the integrity of sensor data. Forged data can be injected in the network. The vulnerabilities' present in WSN can cause harm or loss of data. However system confidentiality is there in position still there is an opportunity to facilitate the data integrity can be jeopardized. Data Integrity is more needed in WNSs to ensure the consistency of data and concern to the probability to validate that the coming message is not tempered and distorted.
- Data Availability: Availability is key importance for keeping up a prepared system and it decides if a node can utilize the assets and whether the network is available for data communication. If the base station or cluster head is not responding, the performance of entire WSN is affected.
- Time Synchronization: The majority sensor networks applications are driven by time synchronization. This time synchronization may be required by sensors to determine the process to process adjournment of a message. A more community oriented WSN may involve collective synchronization for successive applications.
- Data Freshness: Data freshness ensures availability of most current data and nobody is allowed to broadcast old messages again and again. Though data confidentiality and data integrity may be in place still freshness of data is more important. In addition to this, to ensure data freshness, a time- related counter can be prolonging into the packet.
- Secure Localization: A WSN planned to build up for difficulty resolve, requires exact position of data in diversity to connect to location of a problem, the adequacy of a WSN will exclusively count on the sensor nodes capabilities. And an assailant is equipped for without trouble control non-verified area data by presentation produced forged signal power, echo signals.
- Self Organization: Basically a WSN normally is an ad-hoc network, in which hubs are self-contained and sufficiently adaptable to act naturally sorting out and self-modify according to various conditions. There is no fix establish infra-structure available with the end goal of system administration in a WSN. This normal component conveys an awesome analysis to remote sensor organize safety measures. If self-affiliation is insufficient in a sensor compose the problem forthcoming concerning due to an attack or even the hazardous condition may destroy.

1.4. ATTACKS AGAINST WSN

Because of the absence of basic security measures and the unreliability of WSNs and channels, the WSNs are more vulnerable against the allkind of attacks like inside and outside attacks. WSN are more inclined to power or other failures, malicious user can attack the WSN since it is substantially fragile. A physical weak node is effortless to attack rather than a classic node because a classic node is difficult to be caught to turn into a mischievous node or by embeddings a mischievous node in the system (Mohammadi, Ebrahimi, and Jadidoleslamy, 2011), (Wang, and Gong, 2011), (Dimitrievski, Pejovska and Davcev, 2011), (Karlof, and Wagner, 2003), (Shi, and Perrig, 2004). Inferable from the communication conditions of the transmission medium, WNSs are vulnerable to a variety of security attacks. WSN are weak network in terms of hardware and software against security attacks as results, of the broadcast character of transmission medium. And hubs are consistently set in a hostile or hazardous condition where they are not physically secured. For a massive incorporation WSN, it is unfeasible to oversee and shield every specific hub from physical or legitimate assault. And these attacks can be classified in diverse type.

1.4.1. TYPE OF ATTACKS AGAINST WSN

WSNs attacks can be classified in various categories depending upon various parameters.

First classification depend on the position of the attacker i.e. outsider and insider attackers. Outside attacks (Wang, Attebury, and Ramamurthy,2006), (Shi, and Perrig, 2004) are characterized by the nodes that does not belong to WSN where as insider attacks are realize by the authentic nodes of a WSN that act in unexpected or legitimate ways.

Second classification is based on the strength of the attacking node. Attack in this classification characterized as laptop-class versus mote-class assault. Laptop-class assault are accomplished by an opponent who exploits extra prevailing devices (e.g., a laptop) to assault a WSN whereas Mote-class attacks are carried out when an opponent assault a WSN by utilizing a couple of sensor nodes whose power is like to the other system nodes.

Third classification is based on the basis of destruction cause by the attacks. This classification categorizes the attacks in two categories named as passive and active assault. Passive assaults are those in which there is no harm to the data. But attacker tries to eavesdrop or observes packets traded inside a WSN. Whereas active attacks tries to modify the information by including a few changes of the information steam or the making of a false stream. This classification is more popular and consider significantly in the security of WSN.

Passive attack includes monitoring and listening of the communication channel or data stream by legitimate attackers. The common type passive attacks that listed in literature are:

- Monitor and Eavesdropping: Adversary could without any difficulty determines the communication content by inquisitive to the data.
- Traffic Analysis: However as the messages that are transmitted are encrypted regardless it has a vast authentic examination of the communication framework and the sensor conduct can possibly disclose satisfactory data to authorize a challenger to make malicious harm to the WSN.
- Camouflage Adversaries: Adversary node or nodes can compromise the other nodes to put out of sight in the WSN. These nodes are able to duplicate as an ordinary node to draw the packets conducting the isolation analysis by misroute the packets.

In active attacks the information stream in the communication channel can be monitored, listened to and modified by attackers. The following active attacks are:

a) Spoofing, altering or replaying attack

These attacks focuses on the data transmitted over the communication channel. With the help of spoofed information, an adversary may tries to generate routing loops in the network, traffic can be reorganized, transmission routes can be expand and reduce, generates fake error messages, network can be portioned, and end to end latency can be increased. The only solution to spoofing altering and replaying is authentication i.e., routers can check the authenticity of the message.

b) Energy drain attack

Duplicate reports can create false alerts in the system that results in wastage of network response efforts, and that in turns drain the energy of the powerful systems. In any case, the attack is possible given that the attacker node has adequate amount of energy to communicate in the WSN. The foremost motive of this attack is to make WSN unresponsive due to energy drainage and attacker can get hold of the system and reconfigure the network.

c) Node replication attack

In node replication attack, attacker seeks to accumulate numerous hubs using identicalidentity at extremely unexpected places of the predominant WSN.

d) Selective forwarding attack

Selecting forwarding attack is more common type of assault in which a multi- hop mode of correspondence where a adversary node could decline to forward certain messages and effectively disappear them, verifying that they cannot be routed any more in the network.

Source: Unsal Emre and Çebi Yalçın, (2013).

.

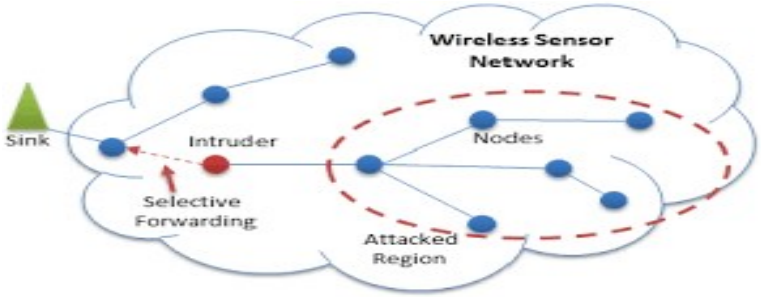


Fig. 1.3 Selective forwarding attack

e) Sinkhole attack

By sinkhole attack, someone aim is to endear the entire transmitted data from a specificspace using compromised node as intermediate node to destination. An attacked node that is put at a place build a great “sphere of influence” that the traffic is distracts from the true route. The attacker tries to focus on an area where traffic is more so that it draws maximum traffic from compromised mode. It is presumably nearer to the task manager so that compromised node might be alleged as a task manager.

Source: Keerthana G., and Padmavathi G., (2015).

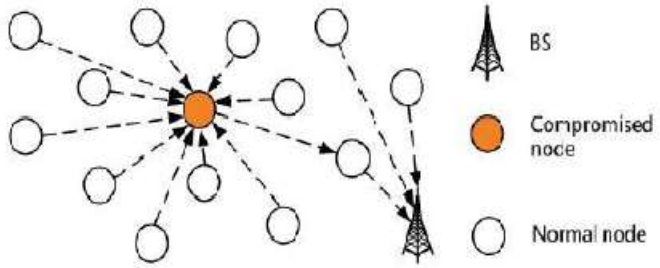
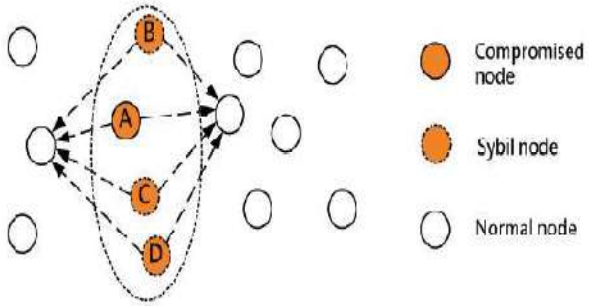


Fig. 1.4 Sinkhole attack

f) Sybil attack

Communication protocols expect that every node in the network has unique identity and the nodes will appear to be in numerous spots at different time. Attacker will misuse these identities by appearing at mark at same time. This might happen because of duplicate identities of nodes settled at the sting of correspondence differ. Various identities might be involved inside the WSN either stealing or fabricating the identities of valid nodes.

Source: Singh, Singh, and Singh, (2016).



.
Fig. 1.5 Sybil attack

g) Black-hole attack

This attack configure a hub in route of sink and destroy the actual genuine route and tries to controlled the WSN by publicizing itself in light of the way that the smallest route. Someone drops packets returning from definite sources inside the framework.
Source: Unsal and Çebi, (2013).

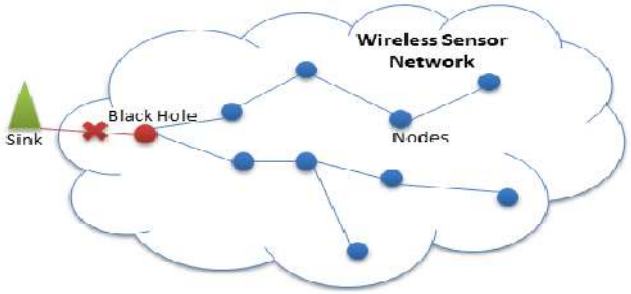


Fig1.6 Black-hole attack

h) Wormholes attack

In this attack someone may succeed upon nodes organization would unremarkably be different bound from a base station that they are very near to destination by new route. The best instance of this assault is to have a malicious node that as intermediate node and sending data between two legitimate nodes. Wormholes generally prevail upon far off nodes that they are neighbors', bringing about swift fatigue of their power assets.
Source: Monika, Kumar and Rishi, (2010).

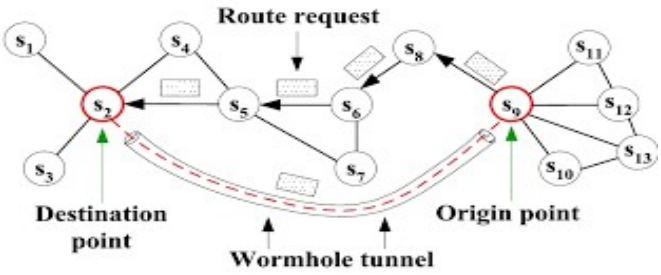


Fig. 1.7 Wormhole attack

i) Hello flood attack

Several protocols formulate nodes to put out hello packets for neighbor discovery. And nodes getting these packets consider them normal traffic from the correspondent. A laptop-class assailant through huge broadcast power may overcome upon each sensor node inside the system that someone is its neighbor, so every one of the nodes can answer the hello message and consume their energy in replying these messages. The consequences of hello flood attack are that both resources and nodes are busy in sending hello messages.
Source: Dahane, Berrached and Loukil, (2016).

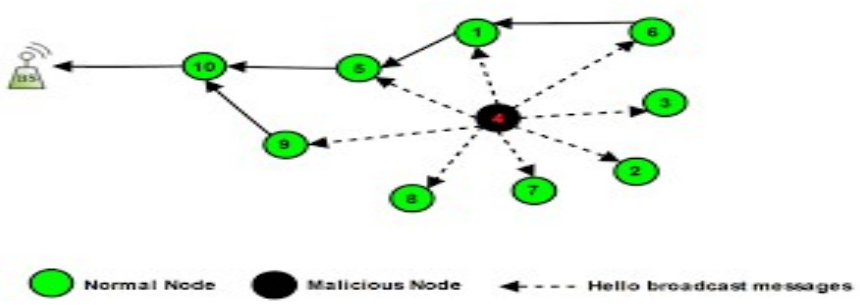


Fig. 1.8 Hello flood attack

j) Denial of Service attack (DOS)

DOS attack is the most common active attack in which attacker attempt to make services unavailable. A DOS attack is an endeavor to formulate a WSN or some other asset inaccessible to legitimate users. Generally, this attack is viewed as a problem of computer network; however for a single CPU also it is very well may be available among different assets. The motive or target of DoS may vary from person to person however by and large; it expects to keep a few administrations from working proficiently either incidentally or inconclusively.Generally, a DoS attack engage the victim by in excess of the peak correspondence demands and because of this the focused on framework cannot react the real clients at all or reacts in all respects gradually, dissipate its viability. There are some of the symptoms by which the presence of DoS can be identified such as network performance goes slow, some of the targeted web sites become unavailable, increase in spam emails, loss or delay of packets and their acknowledgement. Basically the reasons for DoS attack can be of any types according to the type of destruction it does. Major reasons are consumption of resources like memory space, processor time, bandwidth etc, deletion or alteration of routing table data, disrupted state information, and destruction of physical components, and obstruction in the communication channels. Due to the disseminated environment of DOS attacks; it is immensely difficult to decide such malevolent conduct utilizing conventional IDS in WSNs.

Fouth classification of attacks is based on host and network in host based attack, attacker targets a host where as in network based attacks, attacker targets the whole network.

Host-based attacks can be further categorized as (Law, 2005):

- User compromise: This includes trading off the clients of a WSN, e.g. by steal the clients' informative information.
- Hardware compromise: This encompasses messing through the equipment to separate the program code, information and keys put away inside a sensor node. The assailant may moreover endeavor to stack its procedure in the jeopardize sensor node.
- Software compromise: This encompasses cracking the product functioning on the sensor nodes and probability are the working framework or potentially the functions working in a sensor node are assailable against well-known exploit.
- Network-based attacks can be viewed as (Law, 2005) either layer-specific jeopardize or protocol-specific jeopardize. This incorporates assaults on data during transmission. Protocol deviation: while attacker try to turns into an insider node of the WSN, and aggressor's to select an vulnerable favorite position meant for itself in the use of the system, the aggressor shows critical influenced process and process that find missing from the intended functioning of the protocol.

1.5. SECURITY MECHANISMS FOR WSN

To identify, avoid and recover from the various security attacks good security mechanisms are used and to counteract malicious attacks a broad range of security mechanisms can be invented.

- Key Establishment and Trust Setup: Due to restricted computational power of WSN the public key cryptographic algorithms are not a feasible solution and the most important is the formation of cryptographic keys in WSN environment. Key-establishment methods should be scale to systems with large number of nodes.
- Confidentiality and Authentication: The majority of the WSN applications oblige reinforcement opposed to eavesdropping on the network, malware injections, and information alteration. Most of the WSNs that are to be preferred to employ link layer cryptography, because of the successive simplicity of organization.
- Secure routing: As WSN routing protocols go through from numerous security vulnerabilities but routing and data transmit is a vital study designed for simple messaging in WSN.

- Privacy: The WSN might also have privacy concerns as faced by other conventional networks, originally the WSNs are use for authorized principle might later be used in unexpected way. On condition that realization of the behavior of sensor nodes and transmitted information accretion is predominantly significant.
- Robustness to message:Robustness of WSN can be enhanced by optimization of networks topology or by securing its weakness.
- Intrusion Detection System (IDS): These security components mentioned above cannot alone ensure ideal security for WSN. Encryption and authentication are insufficient for ensure information security. They can only act as first line of defense. To secure WSN a strict and strong security mechanism is required which includes components for recognizing, responding and generating alerts on interruptions. In WSN security mechanisms implemented to secure data aggregation protocols and routing protocols are designed early so as to restrain an aggressor from breaking the security of the system. An Intrusion Detection System (IDS) is module which monitors a host, system or a network for doubtful activities during the data transmission. Patterns outside normal and expected conduct are termed as intrusion, which depends on the possibility that there exists a recognizable difference in the behaviors of legitimate user and an intruder in the system to such an extent that IDS can counterpart those pre-programmed or most likely intelligent guidelines. An IDS is normally deliberate as the most reliable second line of defense, because of high precision against internal and external attacks. This system permits distinguishing unusual or suspicious stream of transmitted data from the impart target and generate alert when interruption is occur. Comparative to cryptography it is emphatically that IDS can counter for both internal and external attacks. Researches that are working in the domain of application of the IDS' change especially in ad hoc networks, where few subjects were explored in light of its constrained energy and computing storage capacity can be considered for WSNs.

REFERENCES

1) Crow Brain P., Widjaja Indra, Kim Geun Jeon and Sakai Prescott T., (1997), "IEEE 802.11 Wireless Local Area Networks", IEEE Communication Magazine, **35**, pp 116-126.

2) Bisdikian Chatschik, (2001), "An Overview of the Bluetooth Wireless Technology", IEEE Communication Magazine, **39**(12) pp. 86-94.

3) Corson S., and Macker J., (1999), "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501.

4) Olariu Stephan, (2005), "Information Assurance in Wireless Sensor Networks", Sensor network research group, Old Dominion University, in proceeding of: 19th International Parallel and Distributed Processing Symposium (IPDPS 2005), Denver, CO, USA.

5) Karp, and Kung H. T., (2000), "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks",Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 243–254.

6) Yick J., Mukherjee B., and Ghosal D., (2008), "Wireless Sensor Network Survey," Elsevier's Computer Networks: The International Journal of Computer and Telecommunications Networking, **52**(12), pp. 2292-2330.

7) Raghunathan V., Kansai A., Hse J., Friedman J., and Srivastava M., (2005),"Design Considerations for Solar Energy Harvesting Wireless Embedded Systems", IPSN '05: Proceedings of the 4th international symposium on Information processing in sensor networks, pp. 457–462.

8) Zhang P., Sadler C.M., Lyon S.A., and Martonosi M., (2004), "Hardware Design Experiences in ZebraNet", Proceedings of the Second International Conference on Embedded Networked Sensor Systems.

9) Roundy S., Rabaey J.M., and Wright P.K., (2004), "Energy Scavenging for Wireless Sensor Networks with Special Focus on Vibration", Springer-Verlag, New York, LLC, pp. 189-190.

10) Rahimi M., Shah H., Sukhatme G.S., Heideman J., and Estrin D., (2003), "Studying the Feasibility of Energy Harvesting in Mobile Sensor Network", in: Proceedings of the IEEE International Conference on Robotics and Automation, ICRA, **1**, pp. 19–24.

11) Kansai, and Srivastava M.B., (2003), "An Environmental Energy Harvesting Framework for Sensor Networks", in: Proceedings of the International Symposiumon LowPower Electronics and Design, pp. 481–486.

12) Mohammadi S., and Jadidoleslamy H., (2011), "A Comparison of Transport and Application Layers Attacks on Wireless Sensor Networks," International Journal of Information Assurance and Security, **6**, pp. 331-345.

13) Guorui Li, Jingsha He, and Yingfang Fu, (2008),"Group-Based Intrusion Detection System in Wireless Sensor Networks", Computer Communications, **31**(18), pp. 4324-4332.

14) Wazid Mohammad, and Das Ashok Kumar, (2016),"An Efficient Hybrid Anomaly Detection Scheme Using K-Means Clustering for Wireless Sensor Networks", Wireless Personal Communications, **90**(4), pp. 1971-2000.

15) Yick J., Mukherjee B., and Ghosal D., (2008), "Wireless Sensor Network Survey," Elsevier's Computer Networks: The International Journal of Computer and Telecommunications Networking, **52**(12), pp. 2292-2330.

16) Wang Z. L., and Gong G., (2011), "A Survey on Security in Wireless Sensor Networks," Department of Electrical and Computer Engineering, University of Waterloo,Canada, http://www.cacr.math.uwaterloo.ca/techreports/2008/cacr2008-20.pdf.

17) Dimitrievski, Pejovska V., and Davcev D., (2011), "Security Issues and Approaches in WSN, Department of Computer Science," Faculty of Electrical Engineering and Information Technology, Skopje, 2011. http://ict-act.org/ICTInntions.../ictinnovations 2009 submission 21.pdf.

18) Karlof, and Wagner D., (2003), "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, Alaska, pp. 113-127.

19) Shi E., and Perrig A., (2004), "Designing Secure Sensor Networks," Wireless Communication Magazine, **11**(6), pp. 38–43.

20) Wang Yong, Attebury Garhan, and Ramamurthy Byrav, (2006), "A Survey of Security Issues in Wireless Sensor Networks", IEEE Communications Surveys & Tutorials, **8**(2).

21) Unsal Emre and Çebi Yalçın, (2013) "Denial Of Service Attacks In WSN" DOI: 10.13140/2.1.4040.9929.

22) Keerthana G., and Padmavathi G., (2015) "A Study on Sinkhole Attack Detection using Swarm Intelligence Techniques for Wireless Sensor Networks", International Journal of Computer Science and Information Technology & Security, **5**(5), pp. 376-380.

23) Singh Rupinder, Singh Jatinder, and Singh Ravinder, (2016)," TBSD: A Defend Against Sybil Attack in Wireless Sensor Networks", International Journal of Computer Science and Network Security, **16**(11), pp. 90-99.

24) Monika, Kumar Mukesh and Rishi Rahul, (2010) "Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review", International Journal of Computer Applications, **12**(2), pp. 37-43.

25) Dahane Amin, Berrached Nasr-Eddine and Loukil Abdelhamid, (2016),"Safety of Mobile Wireless Sensor Networks Based on Clustering Algorithm" DOI: 10.4018/IJWNBT.2016010105.

26) Law Yee Wei, (2005), "Key Management and Link-Layer Security of Wireless Sensor Networks", Ctit Ph.D. -Thesis Series, Series Number: 1381-3617, Ctit Number: 05-75.