International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-6)

Research Article

June 2015

WSN Security & Threats: A Survey

Anupriya
CSE Department, Kurukshetra University,
Kurukshetra, Haryana, India

Abstract—

This paper puts a light on the security challenges and threats in wireless sensor network. This network follows the TCP model so different kinds of attack are for different layer and still research is going on for a universal security mechanism. Some cross layer mechanisms also exist. This paper studies those mechanisms and provides a platform for our future research.

Keywords: WSN, JTAG, OSI

I. INTRODUCTION

Efficient design and implementation of wireless sensor networks has become a hot area of research in recent years, due to the vast potential of sensor networks to enable applications that connect the physical world to the virtual world. By networking large numbers of tiny sensor nodes, it is possible to obtain data about physical phenomena that was difficult or impossible to obtain in more conventional ways. In the coming years, as advances in micro-fabrication technology allow the cost of manufacturing sensor nodes to continue to drop, increasing deployments of wireless sensor networks are expected, with the networks eventually growing to large numbers of nodes. Potential applications for such large-scale wireless sensor networks exist in a variety of fields, including medical monitoring, environmental monitoring, surveillance, home security, military operations, and industrial machine monitoring.

When designing network protocols for wireless sensor networks, several factors should be considered. First and foremost, because of the scarce energy resources, routing decisions should be guided by some awareness of the energy resources in the network. Furthermore, sensor networks are unique from general ad hoc networks in that communication channels often exist between events and sinks, rather than between individual source nodes and sinks. The sink node(s) are typically more interested in an overall description of the environment, rather than explicit readings from the individual sensor devices. Thus, communication in sensor networks is typically referred to as data-centric, rather than address-centric, and data may be aggregated locally rather than having all raw data sent to the sink(s). These unique features of sensor networks have implications in the network layer and thus require a re-thinking of protocols for data routing. In addition, sensors often have knowledge of their own location in order to meaningfully assess their data. This location information can be utilized in the network layer for routing purposes. Finally, if a sensor network is well connected (i.e., better than is required to provide communication paths), topology control services should be used in conjunction with the normal routing protocols.

As sensor networks are expected to scale to large numbers of nodes, protocol scalability is an important design criterion. If the sensors are managed directly by the base station, communication overhead, management delay, and management complexity become limiting factors in network performance. Clustering has been proposed by researchers to group a number of sensors, usually within a geographic neighborhood, to form a cluster that is managed by a cluster head. A fixed or adaptive approach may be used for cluster maintenance. In a fixed maintenance scheme, cluster membership does not change over time, whereas in adaptive clustering scheme, sensors may change their associations with different clusters over time as shown below.

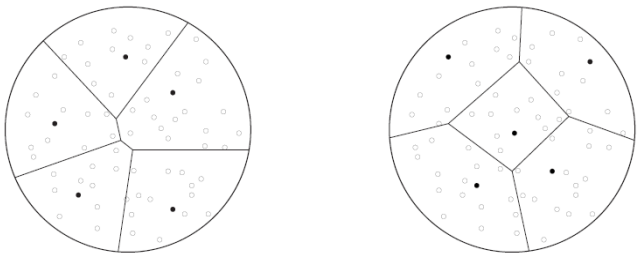

Figure 1.1: Adaptive clustering of the network.

Clustering provides a framework for resource management. It can support many important network features within a cluster, such as channel access for cluster members and power control, as well as between clusters, such as routing and code separation to avoid inter-cluster interference. Moreover, clustering distributes the management responsibility from the base station to the cluster heads, and provides a convenient framework for data fusion, local decision making and local control, and energy savings.

II. THREATS IN WIRELESS SENSOR NETWORK

Recently, the world is becoming more interconnected with the advancement of semiconductor devices which drive faster Internet and new networking technology in smaller devices. Personal, commercial, military, and government information on networking infrastructures worldwide is increasing every day [24]. Hence, to secure any information in a network the security issue became a major concern both in wired and wireless networks. Wired and wireless networks may achieve the same goal but they are not the same at the technical level. Thus, the security mechanisms are different in wireless networks because of the nature of wireless communications. Wired networks connected via Ethernet normally are reasonable secure for the communication media by its nature as its dedicated connection. Whereas, wireless communications require security configuration to prevent anyone within the transmission range of the router, switches and bridges from connecting to the network as the transmission media is shared [35]. Thus, malicious deeds can easily happen, such as hacking of networks. WSN is another paradigm of wireless networks. A highly distributed network indicates that it is possible to work autonomously in a harsh environment. For example, a large number of sensors are deployed to monitor specific phenomena. Considering the application for environment monitoring WSNs are organised in two structures based on underlying topology: (i) flat and (ii) hierarchical. Based on the application the topology can decided. In flat structures all sensor nodes have essentially same role to perform. Hierarchical structures assign different roles to sensor nodes; it is done by clustering the network. During the data collection and communication any significant or insignificant role performed by the low cost sensor nodes needs to transfer the meaningful information to the sink, thus security provisioning is essential. To develop the security mechanism for WSNs, it is necessary to understand threats, security requirements, challenges as well as the types of attacks that involve in WSNs.

The wireless network transmission medium has a broadcast nature. Hence, it is more susceptible to security attacks compared with the traditional wired network. In wireless sensor networks, nodes can be deployed randomly in the hostile environment so an adversary can easily attack the targeted WSNs [18]. The security of WSNs can be investigated in different perspectives. This work formulate a threat model that distinguishes two major types of attacking classes [28 – 30] namely, (i) based on attacker's location, and (ii) based on attacker's strength. In this research, the work focused on the internal attacks of a WSN. In order to clarify all those mentioned terminologies, the definitions are described below: Attacks based on attacker's location Attacks based on attacker's location ocation: Based on knowledge and privileges of the attacker, attacks can be categorized as insider (internal) and outsider (external) depending on whether the attacker is a legitimate node of the network or not [22]. Attacks can also be classified as passive and active attacks.

Internal attacks: When a legitimate node of the network acts abnormally or illicitly it is considered as an internal attack. It uses the compromised node to attack the network which can destroy or disrupt the network easily. An adversary by physically capturing the node and reading its memory can obtain its key material and forge network messages. Having access to legitimate keys can give the attacker the ability to launch several kinds of attacks, such as false data injection and selective reporting, without easily being detected. Overall, insider attacks constitute the main security challenge in wireless sensor networks; that is why all of this research focusing this direction, which will be demonstrated in the following Chapters.

External attacks: This attack is defined as the attack performed by a node that does not belong to the network. Obviously, the attacker node does not have any internal information about the network such as cryptographic information.

Passive attacks: The attack does not have any direct effect on the network as it is outside the network. Passive attacks are in the nature of eavesdropping, or monitoring of packets exchanged within a WSNs when the communication takes place over a wireless channel. This type of attack does not create any interruption in communication process. An attacker can inject useless packets to drain the receiver's battery, or it can capture and physically destroy nodes.Usually authentication and encryption techniques prevent such attackers from gaining any special access to the network.

Active attacks: This type of attack involves disruption of the normal activity of the network. It can do information interruption, modification, traffic analysis, and traffic monitoring [13]. Active attacks are jamming, impersonating, and denial of servicing and message replay. Attack based on attacker's strength Attack based on attacker's strength ased on attacker's strength: Attackers may use different types of devices to attack the targeted network; these devices have different computation power, radio antenna and other capabilities. Two common categories have been identified by Karlof and Wagner [19] including laptop-class and mote-class attackers.

Laptop class: To launch an attack, attackers may have access to powerful devices such as faster CPU, larger battery power, bigger memory space, high-power radio transmitter or a sensitive antenna. This hardware device allows a more broad range of attacks which are more difficult to stop. Their goal may be to run some malicious code and seek to steal secrets from the sensor network or disrupt network normal functions. For example, Harting et. al. demonstrated how to extract cryptographic keys from a sensor node using a JTAG programmer interface in a matter of seconds [14].

Mote-class: Attackers have accessed one or more sensor nodes with the same or similar capabilities like the sensor node deployed in the network. They may try to jam a radio link, but only in the sensor node's immediate vicinity. However, these attacks are more limited since the attackers try to exploit the network's vulnerabilities using only the sensor's node capabilities.

2.1 Nature and Types of Internal Attacks

Simple sensor nodes are usually not well physically protected because they are cheap and are always deployed in open or even in hostile environments where they can be easily captured and compromised. Hence, from a compromised node an adversary can extract sensitive information, control the compromised node, and let the compromised node service the

attacker (adversary). The attacks are involved in corrupting network data, disconnect network communication. The compromised node has the following characteristics [17][18]:

- Compromised node is usually reprogrammed by the attacker by injecting malicious code. Thus, the compromised node seeks to steal information from the sensor network or disrupt the network normal functionality.
- Compromised node uses the same radio frequency as the other normal sensor nodes so that it appears to communicate with normal nodes.
- Deployed normal nodes are authenticated and participate in the sensor network. Since secure communication in sensor networks is encrypted and authenticated using cryptographic keys, compromised nodes with the secret keys of a legitimate node can participate in the secret and authenticated communication of the network.

The compromised nodes are dangerous in a WSN, due to the fact that an adversary can easily access information from compromised nodes such as the cryptographic information, by which a compromised node can gain trust of other sensors. This type of attack is difficult to break or stop. That is why it has become a challenging task to secure WSNs from internal attacks. In many applications, the data obtained from the sensing nodes needs to be kept confidential and it has to be authentic. In the absence of security a malicious node could intercept private information, or could send false messages to nodes in the network. In order to make further investigation for the attacks related to WSNs, in the corresponding sub-sections discussed and took a closer look at some popular attacks. The major attacks this work want to highlight are: Denial of Service (DoS), Worm hole attack, Sinkhole attack, Sybil attack, Selective forwarding attack, Spoofed and altered, or Replayed routing information, Hello flood attack and Flooding attack. Based on the Open System Interconnect (OSI) model the attacks can be tabulated in Table 2.1 [31 - 33]:

Table2.1: various attacks in different layers

A. ***Layer***	*B.* ***Attacks***
C. Physical layer	*D. Jamming, Tampering, Sybil Attack*
E. Data Link Layer	*F. Collision, Sybil Attack, Spoofing and Altering Routing Attack, Replay attack*
G. Network Layer	*H. Internet smart attack, Sybil Attack, Black hole Attack, Spoofing and Altering Routing Attack, wormhole attack, selective forwarding attack, Hello Flood Attack, sink Hole Attack*
I. Transport Layer	*J. Flooding Attack, De synchronization*
K. Application	*L. Spoofing and Altering Routing Attack, False Data Injection*

Denial of Service (DoS) attacks: This attack is an explicit attempt to prevent the legitimate user of a service or data. The common method of attack involves overloading the target system with requests, such that it cannot respond to normal traffic. As a result, it makes the system or service unavailable for the user. The basic types of attacks are: Jamming, Tapering, Collision, Homing and Flooding. If a sensor network encounters DoS attacks, the attack gradually reduces the functionality as well as the overall performance of the wireless sensor network. In WSNs several types of DoS can be performed in different layers which are tabulated in Table 2.2 [34].

Table 2.2: Layer Based DOS Attacks

M. ***Layer***	*N.* ***Attacks***
O. Physical layer	*P. Jamming, Tampering*
Q. Data Link Layer	*R. Collision, Exhaustion*
S. Network Layer	*T. Misdirection*
U. Transport Layer	*V. De synchronization*
W. Application	*X. Path Based DOS*

Jamming: In this attack the attacker attempts to jam the frequencies of the radio used for communication between the nodes in the network. An adversary may use a few nodes in strategic positions to effectively jam most of the communications inside the network. In essence, an attacker needs only a few nodes in order to disseminate a large network.

Tampering: Because of the nature of wireless sensor networks, an adversary could easily get physical access to the sensor nodes. This may enable an attacker to compromise sensor nodes in a DoS like manner.

Collision: In This attack a node induces a collision in some small part of a transmitted packet. The packet will then fail the checksum check, because of the changes brought on by the collision, and the receiver node will then ask for a retransmission of the packet.

Exhaustion: This attack is one of collision attacks which take them a bit further damage WSNs. A malicious node may conduct a collision attack repeatedly in order to exhaust the power supply of the communicating nodes.

Misdirection: In this attack a malicious node that is part of a route can, instead of dropping packets, quite simply send them on a different path which does not exist in a route to the destination. The malicious node may do this for certain packets, or all packets.

Desynchronisation: It can disrupt an existing connection between two end points. Adversary transmits a lost packet with bogus sequence numbers or control flags to degrade or prevent the exchange of data.

Wormhole Attack: In this attack, a malicious attacker receives packets from one location of a network, forwards them through the tunnel and releases them into another location. Hence, the attacker is able to send packets, routing information, ACK etc., through a link outside the network to another node somewhere else in the same network. The malicious node can achieve the faith of the neighbor node as a legitimate node [15]. This can also confuse routing mechanisms that rely on knowing distances between nodes. A wormhole attack can be used as a base for eavesdropping, not forwarding packets in a DoS like manner, and altering information in packets before forwarding them.

Sinkhole Attack: An attacker gains attraction to surrounding nodes with respect to the routing algorithm through a compromised node [17] [35]. It prevents the base station from obtaining complete and correct data. In this attack, a malicious node advertises a zero cost route through itself. If the routing protocol in the network is a "low cost route first" protocol, like distance vector, other nodes will chose this node as an intermediate node in routing paths. The neighbours of this node will also chose this node in their routes, and compete for the whole bandwidth.

Sybil Attack: The concept of Sybil (or multiple-identity) attacks was first proposed by Douceur in P2P networks [35], and it is defined as a single node has multiple identities to disrupt the accordance among the entities and physical devices in a networks. This attack poses a serious threat for damage to WSNs' integrity. A malicious node forges multiple identities to mislead the network and let the neighbor nodes to believe that they have several trusted neighbors. This attack targets fault tolerant schemes such as distributed storage, dispersity, multipath routing and topology maintenance. This attack is especially confusing to geographic routing protocols as the adversary appears to be in multiple locations at once. Hence, it is very hard to identify the position as the malicious node could appear in more than one place at the same time.

Selective Forwarding Attack: In a simple form of selective forwarding attack, malicious nodes try to stop the packets in the networks by refusing to propagate any further [31]. Another variance of selective forwarding attacks is to delay packets passing through the nodes, creating the confused routing information between sensor nodes. Even though the protocol is completely resistant to the sinkholes, wormholes, and the Sybil attack. If a compromised node is strategically located near the source or a base station there is a significant probability of including the compromised node on a data flow to launch this type of attack. However, such an attacker takes the risk that neighboring nodes will conclude that it has failed and take other route.

Spoofing Attack: In an open nature, the characteristics of a wireless medium are easy for any malicious node to monitor the communications to find the layer to Media Access Control (MAC) addresses of the other entities in this network. This can have a serious negative impact on the network performance as well as facilitate many forms of security weaknesses. In this attack, a malicious node is able to create routing loops, wormholes, black holes, partition the network, by spoofing, altering or replaying routing information.

Hello Flood Attack: Hello Flood Attack is introduced in. The malicious nodes broadcast hello messages to announce their presence to the neighboring nodes. The node receiving the message assumes that the malicious node is within its range or a neighbor. An attacker with a high powered antenna can convince every node who receives "hello" in the same network which means this node is their neighbor. Hence, the malicious node can deceive other nodes to believe that a normal node is malicious. Nodes at a large distance from the attacker will be sending their messages to an out-of-reach malicious node that can disrupt the network by simply decreasing traffic load and make communications in a state of confusion. This form of attack is specifically designed against routing protocols that are dependent on localized information. All of the above mentioned attacks have the common purpose that is to compromise the integrity or workability of the network that they attacked. In order to ensure the network functions as originally designed a network needs to be saved internally and externally. This research work will need to understand the internal attacks of WSNs. As mentioned in the paragraphs, this thesis highlights internal attacks and discussion about external attacks is outside the scope of this thesis even it is equally important. For meeting up security the next sub section presents related suggestions for this research focus, internal attacks.

III. SECURITY CHALLENGES

The critical goal of WSNs security is to protect the wireless sensor networks from any types of attack. The different application scenarios presented in the earlier section point out that WSNs may have very different properties. Thus, considering the generic security requirements and application scenario the algorithm is developed to secure a WSN. The major properties that made the security mechanism challenging in WSNs are resource constraints, operational environment and unreliable communicatio, which are discussed below. Resource constraint Resource constraints: it is commonly assumed that sensor nodes are highly resource constrained. For an example, the Berkeley MICA2 motes and TMote mini, are presented in Table 1.3 [36][37]. Thus, security protocols for WSNs must be executable based on the available hardware and especially must be very efficient in terms of energy consumption and execution time.

Table 1.3: Sensor Platforms

Y. Characteristics	*Z. Mica2*	*AA. TMote mini*
BB. RAM	*CC. 4(Kbytes)*	*DD. 10 (Kbytes)*
EE. Program Flesh Memory	*FF. 128 (Kbytes)*	*GG. 48 (Kbytes)*
HH. Maximum data rate	*II. 76.8 (Kbps)*	*JJ. 250 (Kbps)*
KK. Power Draw: Receive	*LL.36.81 (mW)*	*MM. 57 (mW)*
NN. Power Draw: Transmit	*OO. 87.90 (mW)*	*PP. 57 (mW)*
QQ. Power Draw: sleep	*RR. 0.048 (mW)*	*SS. 0.003 (mW)*

Operational environment: in most WSNs the operation Operational environment: al environment is always assumed to be unattended or even hostile. Since sensor nodes are usually not assumed to be physically protected by some tamper resistant hardware, an adversary is able to physically attack and compromise the nodes. The attackers are not only capable of physically damaging the device, but they can also alter device characteristics and security mechanisms to send out data readings of their choice. Once a WSN is in control, the attackers can do whatever attackers wanted to the node, such as altering the node to listen to information about the network, inputting malicious data or performing a variety of attacks. The above vulnerability can be enhanced by the absence of any fixed infrastructure. In particular, there is no central controller to monitor the operation of a network and identify attack attempts. Thus, even if security mechanisms are deployed, an adversary is able to participate in a network since it has access to all data, such as, cryptographic keys stored on the node can be obtained. Thus, security protocols should be able to operate when the sensor nodes are compromised, which prevents cooperating nodes from taking corrective measures against their corrupt neighbours so that they continue to rely on the fake information being fed to them.

Unreliable Communication: Certainly, the varying nature of the wireless communication medium, which is inherently insecure, poses another threat to WSNs security. Unlike wired networks, where a device has to be physically connected to the medium, the wireless medium is open and accessible to anyone. Therefore, any transmission can easily be intercepted, altered, or replayed by an adversary. The wireless medium also allows an attacker to easily intercept valid packets and inject malicious ones. Moreover, the unreliable transmission in wireless channel may result in damaged packets. If packets meet with others in the middle of transfer, conflicts will occur and the transfer itself will fail. Such a weakness can be exploited by an attacker, with a strong transmitter, who can easily produce interference or jamming of the network. In addition, wireless multi-hop communication can introduce great latency in a network, which makes it difficult to achieve synchronization among sensor nodes. Compromised nodes may be part of a route, enabling them to modify forwarded messages.

IV. LITERATURE REVIEW

G.N. Purohit (2015) dealt with routing protocol that is based on both the issues i.e. coverage and energy, in which we first find the k-mean i.e. the degree of coverage, so that we can use this in the selection of cluster heads in wireless sensor network by using Genetic Algorithm for increasing network lifetime and coverage. For cluster head selection each node evaluates its k-mean and energy by internal function which used as fitness function in genetic algorithm. To increase the network lifetime, we propose an energy efficient coverage aware routing protocol for wireless sensor network for randomly deployed sensor nodes. Some of the routing protocol is based on energy efficiency and some are based on coverage aware. Umamakeswari Arumugam (2015) proposed an Intrusion Detection System (IDS) mechanism to detect the intruder in the network which uses Low Energy Adaptive Clustering Hierarchy (LEACH) protocol for its routing operation. The detection metrics, such as number of packets transmitted and received, are used to compute the intrusion ratio (IR) by the IDS agent. The computed numeric or nonnumeric value represents the normal or malicious activity. As and when the sinkhole attack is captured, the IDS agent alerts the network to stop the data transmission. Thus, it can be a resilient to the vulnerable attack of sinkhole. Mahdi Shahedi (2015) detected the area in the network where a sinkhole attack has occurred there by considering the energy consumption model in the network. An entropy-based trust model in which more factors that affect trust computation are introduced. A trust-based routing for providing a high level of security by path selection based on packet trust requirement. So it is needed that a routing protocol classifies the traffic packets according to their requested security and then routs the packets related to each class through the path that fulfills the security requirements of them. This paper mentioned a problem which is a resource efficient security protocol. This means that a trust value is allocated to the area suspected of sinkhole; the area is located by analyzing the energy of networks nodes and the packet is forwarded through low risk paths [32]. K.Muneeswaran (2014) proposed the extended Kalman Filter (EKF) mechanism to filter the false data in sensor network. The false data can be acted by some event namely malicious, emergency event. Malicious event are acted by intruders, and Emergency event are acted by some accident occurrence eg. Fire. Intruders make the sensors to get the false reading therefore EKF mechanism is proposed.

EKF monitors the behaviour of neighbours and predict their future states, each node aims at setting up normal range of the neighbor's future transmitted aggregated values. Using different aggregation functions (average, sum, max, and min), theoretical threshold value is calculated. Combining Cumulative Summation (CUSUM) and Generalized Likelihood Ratio (GLR) detection sensitivity can be increased. Intrusion Detection Modules (IDM) and System Monitoring Modules (SMM) work together in order to provide intrusion detection capabilities for WSNs. EKF address various uncertainties in WSNs and create an effective local detection mechanism. Joseph Rish Simenthy (2014) proposed an advanced Intrusion Detection System. It improves the detection rate and efficiency so that almost all the Intrusions can be detected. Also the system is applicable to small, medium as well as large sized networks. That means it gives a wide range of flexibility in detection of Intrusions compared to the other existing systems. Also the energy efficiency and the system life time is greatly improved. Quazi Mamun (2014) presented a model in his paper, which used a Voronoi diagram based network architecture. The network architecture, which deploys mobile data collectors (MDCs), ensures the compatibility of the anomaly detection model for the resource constrained WSNs, and warrants data integrity between the MDCs and the LNs. A sensor node exhibits anomaly in behaviour due to its dying energy level or being compromised by the intruders. The node showing anomalous behaviours being a leader node (LN) of a cluster/group multifolds the vulnerability problem. P.PRIYADHARSHINI (2014) presented Trust Based Neighbor Weighted Voting Scheme to strengthen intrusion detection in WSN. It evaluates the dynamic radio range of neighbor nodes. Weight threshold is evaluated for marking the sensor node as normal node and malicious node. Wireless sensor networks (WSNs) deployed in unattended environment energy recharging is difficult. WSN satisfy application specific QoS requirements i.e., reliability, timeliness, security and minimize energy consumption to prolong system useful lifetime with limited resources. The drawbacks of existing work include redundancy management scheme that did not addresses heavy query traffic. Ambiguity in multi-path routing decision is due to higher level of intrusion tolerance rate. It discards the communication of internal malicious node by identifying lower weight votes of corresponding sensor node. It governs the best WSN settings in terms of redundancy level used for outsource multipart routing number of weighted votes intrusion invocation interval. WSN lifetime is maximized with trust based weighted voting and handles concurrent higher query traffic. Swati Sharma (2014) did a survey of intrusion detection approaches with advantages. KDD cup data used in every technique which have information of computer networks during normal and intrusive behavior. It contains basically four categories of attacks. GA is used to optimization purpose and fuzzy logic work on approximation rather than precise values. NSLKDD is an advance version of KDD cup data set. It is really important to secure the data from any intrusive attacks so intrusion detection is really very helpful in the field of computer network security. Intrusion detection is the act of detecting unwanted traffic on a network. Many current intrusion detection systems are unable to find unknown attacks.

V. CONCLUSION

Since wireless sensor network because of low cost and low energy sensor nodes, making its importance in variety of applications which includes monitoring, surveillance as well as military applications. Form these application point of view, secure protocol for WSN is mandatory but because of many challenges its still a research area. In this paper these challenges are tried to earth out so that it can help us in finalizing security protocol for further work. Some of latest papers of year 2014-2015's discussion have been also included here. Along with security challenges a thorough discussion of threats in wireless sensor networks are also quoted in this paper along with the vulnerable TCP layer of network.

REFERENCES

[1] G.N. Purohit, "implementation of energy efficient coverage aware routing protocol for wireless sensor network using genetic algorithm."IJFCST, Vol.5, No.1, January 2015.

[2] Umamakeswari Arumugam, "Intrusion Detection Algorithm for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Networks." Journal of Sensors, Article ID 203814.

[3] Mahdi Shahedi, "A Trust Based Routing Protocol for Mitigation of Sinkhole Attacks in Wireless Sensor Networks." International Journal of Information and Education Technology, Vol. 5, No. 7, July 2015.

[4] K.Muneeswaran, "Detection of Intruders in Wireless Sensor Networks Using Anomaly." International Journal of Innovative Research in Science ,Engineering and Technology Volume 3, Special Issue 3, March 2014.

[5] Joseph Rish Simenthy, "Advanced Intrusion Detection System for Wireless Sensor Networks." International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Special Issue 3, April 2014.

[6] Quazi Mamun, " Anomaly Detection in Wireless Sensor Network." Journal of Networks, vol. 9, no. 11, November 2014.

[7] P.Priyadharshini, "Trust Based Voting Scheme and Optimal Multipath Routing for Intrusion Tolerance in Wireless Sensor Network." IJCSMC, Vol. 3, Issue. 2, February 2014, pg.255 – 260.

[8] Swati Sharma, "Recent trend in Intrusion detection using Fuzzy-Genetic algorithm." International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 5, May 2014.

[9] Chandra Prakash, "A Comparative Study Of Intrusion Detection System For Wireless Sensor Network." IJAFRC, Volume 1, Issue 5, May 2014.

[10] DEEPA S, "Trust Management Schemes For Intrusion Detection Systems -A Survey." International Journal of Advanced Computational Engineering and Networking, Volume-2, Issue-8, Aug.-2014.

[11] Mohammad Abu Alsheikh, "Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications." IEEE Communications Surveys and Tutorials. 2014.
[12] Sathyabama.B, "Energy Efficient Voting Based Intrusion Detection Techniques in Heterogeneous Wireless Sensor Network." IJCSMC, Vol. 3, Issue. 1, January 2014, pg. 374 – 380.
[13] K.Kumaresan, " Weighted Voting based Trust Management for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks." IJAFRC, Volume 3, Issue 6, Nov 2014.
[14] Sneha Dhage, " Intrusion Detection & Fault Tolerance in Heterogeneous Wireless Sensor Network: A Survey." International Journal of Scientific and Research Publications, Volume 4, Issue 2, February 2014.
[15] Jaime Lloret, "Intrusion Detection Algorithm Based on Neighbor Information Against Sinkhole Attack inWireless Sensor Networks." The Computer Journal Advance Access published May 13, 2014.
[16] Suhasini Komara, " Sinkhole Attack Detection In Hierarchical Sensor Networks." International Journal of Scientific & Engineering Research, Volume 5, Issue 9, September-2014.
[17] Junaid Ahsenali Chaudhry, "Sinkhole Vulnerabilities in Wireless Sensor Networks." International Journal of Security and Its Applications Vol.8, No.1 (2014), pp.401-410.
[18] Nabil Ali Alrajeh, "Secure Ant-Based Routing Protocol for Wireless Sensor Network." International Journal of Distributed Sensor Networks ,Volume 2013, Article ID 326295, 9 pages.
[19] Udaya Suriya Rajkumar, "A Leader Based Monitoring Approach For Sinkhole Attack In Wireless Sensor Network." Journal of Computer Science 9 (9): 1106-1116, 2013.
[20] R˘azvan Rughinis, "Adaptive Trust Management Protocol based on Intrusion Detection forWireless Sensor Networks." International Journal of Scientific & Engineering Research, Volume 1, Issue 9, September-2012.
[21] Sibaram Khara, "K-Means Clustering In Wireless Sensor Networks." Fourth International Conference on Computational Intelligence and Communication Networks, 2012.
[22] Shio Kumar Singh, "Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks." International Journal of Advanced Science and Technology Vol. 30, May, 2011.
[23] Ioannis Krontiris, "Cooperative Intrusion Detection in Wireless Sensor Networks." International Journal of Distributed Sensor Networks, 2011.
[25] Md. Safiqul Islam, "Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches." International Journal of Advanced Science and Technology Vol. 36, November, 2011.
[26] C. Kolias, "Swarm intelligence in intrusion detection: A survey." IJAFRC, Volume 2 Issue3, Nov 2011.
[27] Michael Krishnan, "Intrusion Detection in Wireless Sensor Networks." ACM SENSYS, November 2010.
[28] Marcelo H.T. Martins, "Decentralized Intrusion Detection in Wireless Sensor Networks." Q2SWinet'05, October 13, 2010.
[29] Ioannis Krontiris, "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks."International Journal of Advanced Science and Technology Vol. 36, November, 2009.
[30] D. Sheela, "A Recent Technique to Detect Sink Hole Attacks in WSN." Journal of Computer Science 9 (9): 1106-1116, 2005.
[32] K. Sharma and M. K. Ghose, "Wireless Sensor Networks: An Overview on its Security Threats," IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs; CSE Department, vol. 1, no. 1, pp. 42–45, 2010.
[33] H. K. D. Sarma and A. Kar, "Security Threats in Wireless Sensor Networks," in Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International, Oct., pp. 243–251.
[34] H. Ghamgin, M. S. Akhgar, and M. T. Jafari, "Attacks in Wireless Sensor Network," vol. 5, no. 7, pp. 954–960, 2011.
[35] Padmalaya Nayak, V. Bhavani," Impact of Black Hole and Sink Hole Attacks on Routing Protocols for WSN" International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 4, April 2015
[36] M. Corporation, "Data sheet Tmote sky." Moteiv Corporation, 13-Nov-2006.

