International Journal of Engineering & Technology, 7 (2.33) (2018) 89-94

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Wireless sensor networks security issues and challenges: A survey

Vikhyath K. B [1], Dr. Brahmanand S. H [2]

[1] *Department of Information Science and Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka-572105, India*
[2] *Department of Computer Science and Engineering, GITAM School of Technology Nagadenehalli, Doddaballapur Taluk Bengaluru Rural District, Karnataka- 561203, India*
**Corresponding author E-mail: Vikhyath059@gmail.com*

Abstract

Wireless Sensor Network (WSN) is a rising technology that offers a great assurance towards a variety of revolutionary applications such as military and public. As wireless sensor networks continue to develop, there is a high importance in security mechanisms. As sensor networks works with responsive data and operate in antagonistic environments, it is crucial to address the security issues. The sensing technology united with wireless communication and processing power makes it rewarding. Due to these computing and inherent constraints in resource, sensor network security has special challenges. The low cost and collaborative nature of the wireless networks (WNs) offers significant advantages upon the conventional communication techniques. The wireless communication technology has several kinds of security threats. The spotlight of this paper is towards addressing the security issues and challenges of WSNs. Here the idea is to identify the threats and security mechanism of wireless sensor networks.

Keywords: *Adversary; Wireless Sensor Network; Security Issues*

1. Introduction

Today Internet has turned out to be one of the essential pieces of our day by day life. It has changed how individuals live, work, play and learn. IOT systems as of now rely primarily on sensors and remote systems that allow remote access to data or application. In any case, IOT offers noticeable assurance in the field of wellbeing mindfulness more than any other area. As a maxim goes "Wellbeing is riches" it is astoundingly pivotal to make Use of the development for better prosperity. Subsequently an IOT system is added, which gives secure wellbeing mindfulness checking. The present patient screen frameworks in healing facilities permit persistent checking of patient imperative signs, which require the sensors to be hardwired to available, screens or PCs near the patient's bed, and limit the patient to the ward assigned by the doctor. Indeed, even subsequent to associating these frameworks to a specific patient, a paraprompt fiasco on account of a human blunder.

Late years have seen a rising enthusiasm for wearable sensors and today a few gadgets are financially accessible [1]-[3] for individual human services, fitness, and action mindfulness. In light of current mechanical patterns, one can promptly envision a period sooner rather than later when your routine physical examination is gone before by a two– three day time of ceaseless physiological checking utilizing economical wearable sensors. Such a problematic innovation could transformatively affect worldwide medicinal services frameworks and radically lessen social insurance costs and enhance speed and exactness for analyze.

2. Literature survey

Wireless Sensor Networks (WSN) is an emerging technology involving distributed sensor nodes through multi-hop routing (Culler & Hong, 2004). Wireless sensor networks gains rapid popularity due to tiny sensing devices. They are the potential low-cost solutions to environmental monitoring, surveillance and target tracking etc (Akyildiz & Su et al, 2002). The communication in wireless sensor networks is done using wireless transceivers, which can monitor noise levels, vehicular movements, lighting conditions, humidity, pressure and temperature (Pathan & Islam et al, 2006).

In general traditional networks support point-to-point or point-to-multipoint data communication. WSNs have the ability to work virtually in any physical environment, where wired connections are impossible. They are deployed to sense, process and disseminate information of any targeted environments. Before network deployment the location of nodes are not specified and this capability allows us to spread them in remote and dangerous areas. In order to protect the nodes, the self organizing protocols and algorithms are used. Basically the battery-operated sensor devices of WSNs are equipped with data processing, computing and data communicating components. Conventional wireless sensor networks are prone to additional threats which results from intrinsic characteristics of sensor nodes such as CPU cycles, battery capacity, memory, deployment environment and, communication bandwidth. Because of these intrinsic properties of sensor nodes traditional security mechanisms for providing authentication, availability and confidentiality are inefficient for wireless sensor networks.

The major challenges for employing efficient security mechanism in WSNs are created by the size, memory, processing power of the

sensors. The lack of power and data storage initiates severe resource constraints in WSNs. Both are major obstacles towards the traditional security implementation techniques (Perrig & Szewczyk et al, 2002).
Considering this many researchers started dealing with the challenges of energy funds and maximize the processing power of sensor nodes. Surveillance and monitoring are the prime factors in controlled environment. Whereas sensor network security becomes extremely important in uncontrolled environment. Even though wireless sensor networks assure large number of applications there are many problems of securing these networks. The major preferences in wireless sensor networks are modelling and routing strategies, yet security issues are of extensive focus. Sensor networks are predominantly prone to several kinds of attacks. They are executed in a variety of ways, most remarkably as DoS attacks, physical attacks, violation of privacy, traffic analysis and so on. Majority of the attacks in opposition to WSNs are due the inclusion of false information by the compromised nodes of the network. A mobile agent-based security system is developed for defending and detecting the false reports by compromised nodes (Brar & Arora, 2013).
In recent times, mobile agent based computing prototype has become an activist in the perspective of wireless sensor networks. A mobile agent is defined as an autonomous software component which acts like a thread or a programming segment. This is self-controlling and migrates among the nodes following an itinerary and carries out the data computation (Chen, Gonzalez & Leung, 2007).
This paper outlines the security issues and challenges of wireless sensor networks and confers the critical parameters. Very first we introduce the obstacles and security requirements of WSNs. Later summarizes the security treats and sufficient defensive mechanisms. Finally, the importance of introducing mobile agent-based software prototype is pointed out.

2.1. Sensor security obstacles

As compared to the traditional network, wireless sensor network has several constraints. Because of this it is hard to directly utilize the existing security mechanisms for WSNs. While developing functional security mechanisms following constraints are considered (Carman, Krus & Matt, 2000).

2.2. Limited resources

Implementation of the security approaches require amount of resources like memory and power. These resources are not adequate in wireless sensors.

- Limited memory and storage space: Sensors have less memory and storage capacity.
- Power limitation: Wireless sensor capabilities have biggest energy constraints.

Unreliable Communication: This is one of the most important threats in sensor network security and network security seriously relies on protocols. This in turn heavily depends on the communication.

- Unreliable transfer: Wireless sensor network uses connectionless environment for packet-based routing which is intrinsically unreliable. Due to the heavy congestion on the channel the packets may get damaged or even the packet loss may occur.
- Conflicts: Even though we have reliable channel, sometimes communication goes unreliable due to WSNs broadcast nature (Akyildiz & Su et al, 2002).
- Latency: Node processing, congestion and multi-hop routing increases the network latency. It makes sensor nodes synchronization bit difficult.

Unattended Operation: The functionality of the sensor network plays a very important role, in making the sensor node unattended for a period of time. Main warnings of unattended sensor nodes are:

- Exposure to physical attacks: Sensor nodes are deployed in adversary dominated environment.
- Managed remotely: Sensor network remote monitoring makes it impossible to identify the issues of physical tamper and maintenance.
- Lack of central management point: Absence of central management point in the distributed sensor network.

2.3. Security requirements in wireless sensor networks

The resource limitations of wireless communications are sensor nodes, size, topology and density of the network. These are of high security challenges in WSNs. Ultimate security requirements of WSNs are authenticity, integrity and confidentiality.

2.4. Cryptography

Traditionally developed encryption-decryption techniques are not feasible enough to use directly on WSNs. Some critical questions like how keys are generated, managed and revoked will arise while applying encryption and decryption techniques to WSNs.
Encryption schemes in WSNs require transmission of extra bits that consumes more power from the tiny sensors. Extra processing power, memory and battery are the basic parametric resources which improves the longevity of the sensors (Perrig & Szewczyk, 2002). This type of security schemes also increases jitter, delay and packet loss in WSNs (Saleh & Khatib, 2005). For the most secured communications of the WSNs all the messages are encrypted and authenticated. Security attacks on the flow of information can be prevalent. Due to uncontrolled node of environments and nature of wireless channels, the information is vulnerable to modification. An adversary can make use of any kind of cryptographic impairments for modification of the data and make information unavailable.

2.5. Steganography

As cryptography deals with hiding the message content, steganography deals with hiding the message existence (Carman, Krus & Matt, 2000). The art of steganography deals with embedding a message within a multimedia data like image, audio and video. Steganography and multimedia processing are not related to securing wireless sensor networks because of the insufficient sensor resources. Basic security requirements of WSNs are data availability, confidentiality, authentication, integrity and nonrepudiation.

2.6. Data availability

Modifying the legacy encryption schemes to work within the WSN is complicated and expensive. Few approaches enforce severe limitations on the data access to simplify the algorithms. These approaches reduce the sensor networks availability for the below reasons:

- Additional computation and communication consumes extra energy.
- The availability of the network is greatly threatened by single point failure.

2.7. Data confidentiality

Is the most significant issue in network security. Confidentiality in the sensor networks relates to the following:

- A sensor network should not disclose the data to any neighborhoods. Example like military applications requires high confidentiality in data storage.
- For sensitive data communication having a secure channel is highly important.
- Sensor information is encrypted to safe guard against the traffic analysis.

- Thus, confidentiality is achieved by encrypting the sensitive data by sharing the secrete key between sender and recipient (Kurak, & McHugh, 1992).

2.8. Data integrity

Even though, the confidentiality protects the information from the adversary, it doesn't mean that information is secured. Attackers have the ability modify the information. A malicious node may send the manipulated data to the original receiver. In harsh communication environment, the data loss may occur even in the absence of the malicious node. The received data has not been altered in transit can be assured by data integrity.

2.9. Authentication

An attacker not only has the capability to change the data packet. Even it has the ability to modify the entire data stream by adding the extra packets. Therefore the duty of the receiver has to ensure the correct source. While constructing the sensor networks, authentication process is essential for many applications. Symmetric encryption mechanism assures the data authentication in case of two-party communication. Message authentication code is calculated by sharing the secret key between sender and receiver.

2.10. Data freshness

Though the integrity and confidentiality are assured, we have to make sure regarding the data freshness. This implies that the data is recent and no adversary has replayed with old messages. If the design is using a shared key strategy the freshness requirement is very important. Monotonically counter is incremented with every message and the messages with old counter values are rejected. As per literature we have two types of freshness: weak freshness carries no delay but offers partial message ordering, and strong freshness provides delay estimation and offer a total order (Perrig & Szewczyk, 2001).

2.11. Robustness and Survivability

The sensor networks should be strong enough to withstand the security attacks and even if the attack is successful, the effect must be very less. Vulnerability of a node should not breach the entire network security.

2.12. Security threats in wireless sensor networks

Broadcast nature of the transmission channel makes wireless networks highly susceptible to different types of security attacks. Eavesdropping is easy because of the broadcast nature of the wireless communication. As compared to the guided transmission channel communications over unguided transmission channel is more vulnerable to security attacks. Typical sensor nodes mounted in a large area are liable to security threats. It is highly impractical to scrutinize and guard each and every individual sensor nodes in a network against logical or physical attacks.

Sensor networks predominantly vulnerable to many types of attacks like physical attacks, denial of service attacks, traffic analysis and node replication attack and so on.

Denial of Service Denials of service attacks are formed by the malicious action or accidental failure of nodes. By the transmission of the unnecessary packets, DoS attacks tries to drain the resources available at the victim nodes. Thus legitimate network users are prevented from accessing the service. In an extent Denials of Service can diminishes a network's capacity to provide defined services. DoS attacks are performed in different layers in wireless sensor networks.

Tampering and jamming are at the physical layer, exhaustion and collision are at the data link layer, hello flood ,warm hole, sink hole, sybil attack and selective forwarding are belongs to network layer, malicious flooding belongs to transport layer and clone attack is at the application layer. The defensive technique to prevent DoS attacks includes effective key management schemes, rate limitation, error correction, strong identification and authentication of traffic.

Sinkhole Attack

An adversary draws whole traffic towards compromised node. A metaphorical sinkhole is created as adversary draw traffic from specific region through a compromised node, which makes entire traffic, has to go through an adversary. This attack can even facilitate other kind of attacks like selective flooding and be able affect the nodes located at far away distance to the base station. Figure 1 depicts the abstract presentation of a sinkhole attack.

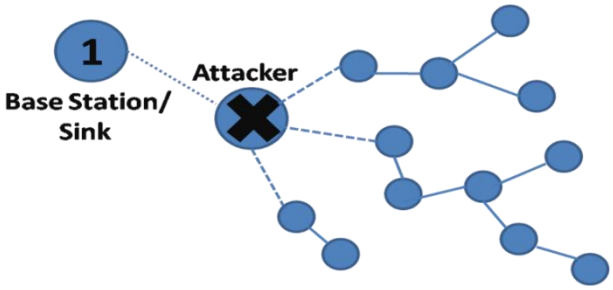

Fig. 1: Sinkhole Attack.

Cloning Attack: This acts like a starting point to span various dangerous attacks. In cloning attack environment an adversary with a compromised node credentials secretly launch the replicas of the node into the network. As these replicas are used to introduce different types of attacks the aim of the sensor applications are threatened.

Wormhole Attack: In the critical wormhole, attack adversary records the messages at one location of the network and tunnels to another location through a low latency channel. As wormhole attack may not necessitate a compromising node in the network, makes this attack a significant one in WSNs.

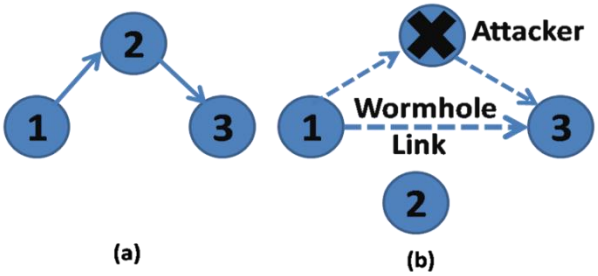

Fig. 2: Wormhole Attack.

Figure two (a and b) depicts the situation of the wormhole attack. When sensor node 1 broadcast the route request packet an adversary captures the packet and forwards to its neighborhood. Once the neighboring node receives this packet, it assumes that it is in the range of node 1 and mark it has its own parent. Thus even though the victim node is multihop at a distance from node 1, the attacker is able to convince that the node 1 is just a single hop apart from them, hence creates a wormhole.

Hello Flood Attack: In this HELLO packets are used like a weapon to deal with tiny sensors of the WSNs. Here adversary with high processing power and transmission range sends HELLO packets to large number of distributed sensor nodes. There by sensors are convinced that the adversary acts like their neighbor. Because of this, while transmitting the data to base station, victim node tries to go across the adversary by thinking that this may be its neighbor and eventually spoofed by the adversary

Sybil Attack: In several scenarios, the tiny sensors of wireless networks have to work collectively to complete a task; hence it demands the functionalities like subtasks distribution and redundancy of information. In such cases, a node can act like another node by stealing the legitimate node identity. In Sybil attack a node fabricates the identities of other nodes (Newsome & Shi et al,

2004). This is very effective against the redundancy mechanisms, data aggregation, routing algorithms and resource allocation (Douceur, 2002). Figure 3 depicts the abstract view of a Sybil attack.

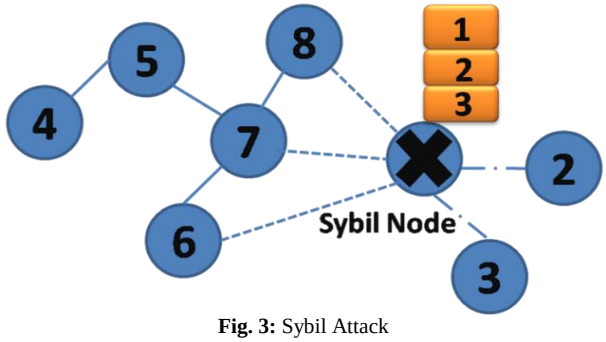

Fig. 3: Sybil Attack

Node Replication Attack: Here by replicating the node ID of the existing sensor node, an attacker can add nodes to the existing networks. Due to such replication of the node, network's performance is severely disrupted. So there may be a chance of packet corruption or misrouting. In turn this results in network disconnection and false readings of the sensors. Once an adversary gains physical accessibility to the whole network cryptographic keys are copied to the replicated sensors and replicated nodes are placed at the strategic points of the network (Parno, Perrig, & Gligor, 2005). Adversary has the ability to manipulate the specific segments of the network by placing the replicated nodes at the strategic points.

3. Layer oriented attacks

Wireless sensor networks are organized by layered architecture. This makes sensor networks highly vulnerable to several different types of attacks.

3.1. Physical layer attacks

As all higher layer functionalities rely on physical layer many attackers targets this layer. Physical attacks on WSNs are like Jamming, node capturing and device tampering, etc (Xu et al, 2005). Due to the lack of the physical control over the nodes its bit difficult to handle the physical attacks rather than software attacks.

- Jamming: This introduces powerful interference to disrupt the availability of the transmission channel.
- Eavesdropping: Without the consciousness of the sender and receiver, adversaries do the WSNs communication channels traffic analysis and gathers the data which can be used later to extract useful information (Franklin, Galil & Yung, 2000).
- Device tampering: This attack leads to modify or damage the sensors physically to harm their service.

3.2. Data link layer attacks

The neighboring nodes coordination is the basic functionality of the link layer protocols to arbitrate the shared channel use. Adversary can violate the coordination rules and create a malicious traffic to disrupt the network operations and makes nodes vulnerable to denial of service attacks. Link layer threats are like traffic manipulation, and identity spoofing.

- Traffic manipulation:
  Adversary transmits the packets exactly at the same time when the authorized user does the transmission to cause the interference. Time synchronization can be done by observing the communication path and doing the calculation based on link layer protocols in effect.
- Identity spoofing:
  Wireless communication broadcast nature makes the identity of the sensor open to all neighboring nodes, including attackers. Due to this an attacker can forge an identity and behave like the different one.

3.3. Network layer attacks

Network layer key concern is to position the destination and finding the optimal route to destination. Attackers can fail the communication by the packets replication and modifying the routing information. WSNs network layer is highly vulnerable to the attacks like false routing, packet replication, sinkhole attack, black hole attack, selective forwarding and wormhole attack, etc.

- False routing: False routing information is enforced to launch the false routing attacks. The different enforcement approaches are like poisoning caches, routing tables, and overflowing the routing tables (Murthy & Manoj, 2004).
- Packet replication: In the packet replication, attackers replicate the earlier received packets. Repeated broadcast of replicated packets consumes large network bandwidth and power of the node which causes the early termination of the network operations.

3.4. Transport layer attacks

An adversary repeatedly makes a new connection request until the resources reach the maximum limit. This leads to the severe resource constraints in legitimate nodes (Raymond & Midkiff, 2008). Transport layer is vulnerable to attacks like flooding and desynchronization attack.

- Flooding attack: These types of attacks take advantage of protocols which maintains information about the connection at both ends.
- Desynchronization attack: An adversary transmits the forged packets with spurious information's like sequence number and control flags to interrupt an active connection.

3.5. Application layer attack

Application layer offers the services to the end users. As such services are time synchronization and data aggregation. Application layer is vulnerable to attacks like data aggregation distortion, clock skewing and selective message forwarding.

- Data aggregation distortion: Data processing is done at the base station, once collected data is given back to the base station by the sensor node. An adversary can change the information to be gathered and make distorted to the final computed results of the base station (Shi & Perrig, 2004).
- Clock skewing: This attack targets the sensors, which necessitate synchronized operations (Yu & Li et al, 2011). An attack desynchronizes the sensors by disseminating the fake timing information.
- Selective message forwarding: This attack is initiated by forwarding the selective messages. To launch this attack in application layer, attacker must be aware regarding the semantics of the payload for selective packet forwarding (Karlof & Wagner, 2003).

4. Countermeasures against the attacks

The main confront in WSNs is to provide efficient security mechanisms, by means of sensor size, processing power, memory and communication capacity (Bojkovic, Bakmaz, & Bakmaz, 2008). Various cryptographic techniques are used for the safe communication over the sensor networks (Priyanka, Tephillah & Balamurugan, 2014). To avoid the attacks that compromise a node in getting access to the entire network, a wide variety of countermeasures and defensive mechanisms (Santhi, R. Sowmiya, 2017) are specified in Table 1.

Table 1: Countermeasures and Defensive Mechanisms for Various Types of Attacks in the Protocol Stack

Protocol stack	Attacks	Effects of attack	Countermeasures against attack	Defensive mechanisms
Physical Layer	Jamming	• Confusion • Packet collision • Resource exhaustion	• Detect and sleep • Route around the jammed region • Spread Spectrum technique for radio communication • Tamper-proof packing	• LEACH (Low-energy adaptive clustering hierarchy)
	Node Tampering	• Hardware damage • Access to higher level by sensitive information extraction	• Effective key management schemes • Camouflage the node •	• Direct Diffusion • SPIN
	Traffic Manipulation	• Time Synchronization • Energy exhaustion	• Misbehavior Detection • Intrusion detection system on each node • cryptography-based authentication schemes • Radio resource testing	• LEACH
Data link Layer	Identity spoofing	• Attacker can forge an identity	• Position verification technique • Code attestation technique • Sequence checking method • Identity-key association technique	• Statistical En-Route • Filtering
	Collision	• Interference • Packet loss	• Error correction codes	• LEACH
	Selective Forwarding	• Packet dropping • Information loss	• Transmission of data through multiple paths • Redundancy and probing technique • Data consistency and network flow information approach	• Multi path routing protocol
	Sinkhole Attack	• Alter the information • Packet drop • Spoofing • Reply old messages • Resource exhaustion	• Hop count monitoring scheme • Mobile agent based approach • Using message digest algorithm • Geographic routing • Authentication • Key management • Encryption • Authentication	• Geographic routing protocol • PRSA
Network Layer	Wormhole Attack	• Information modification • Alter the network topology	• Using synchronized clocks • Using directional antennas • Using multidimensional scaling	• AODV • DSR
	Hello flood Attack	• Data congestion	• Pairwise authentication • Geographic routing • Authenticate two way link before acting on information •	• SPIN • Identity verification protocol • Two way authentication protocol • Three way handshake protocol • probabilistic based protocol
	Sybil Attack	• Node forges the identities of more than one node	• Encryption and authentication schemes avoid outside attacks • Use of public key cryptography avoid insider attacks • Direct and indirect validation	• Merkle hash tree • SIGF • Radio Resource Testing • Random Key Predistribution
Transport Layer	SYN (synchronize) flood	• False routing information	• SYN cookies	• Limiting the number of node's connections • Routing access restriction
	Desynchronization attack	• Disrupts the connection between two legitimate nodes	• Packet authentication • Un-forgeable and strong authentication schemes	• Strong authentication mechanisms • Time synchronization
Application Layer	Overwhelming sensors	• services unavailable to legitimate users by overwhelming the resources	• Sensor tuning • Data aggregation	• SNEP (Secure network encryption protocol) • SPIN (Sensor protocols for information via negotiation)
	Data aggregation	• Incorrect view of the monitored	• False reading detection	• Data integrity protection

distortion	environment • Totally disrupted data aggregation		• Access control
Clock Skeing	• Being out of synchronization • Being unstable • Communication disruption	• Un-forgeable and strong authentication schemes • Misbehavior detection techniques	• Strong authentication mechanisms • Data integrity protection • Data confidentiality protection

5. Conclusion

As WSN continue to evolve and commonly used in several high impact applications, the need for the security mechanisms become very important. WSN suffer a lot from several constraints like processing speed, memory, limited energy, unattended operations and unreliable communication etc. A variety of attacks affect the secure communication. Due to the energy depletion of the nodes network lifetime is reduced.

To uphold the authenticity and data integrity measures are to be taken to resist against the attacks. Even though there are many security mechanisms the important one is the cryptographic techniques and protocols. The fundamental means of providing a security in WSNs is through the way of selecting the best suitable cryptographic technique.

In this paper, a detailed survey is given on sensor security obstacles, security requirements of WSNs, threats in wireless sensor networks, layer-oriented attacks, countermeasures against the attacks and cited some important research issues. Anticipation to the study of this paper, the readers can have an enhanced view of various kinds of attacks, countermeasures and, defensive techniques of WSNs..

References

[1] Akyildiz. I. F., Su. W., Sankarasubramaniam. Y. and Cayirci. E. (2002). A survey on sensor networks. *IEEE Communications Magazine, 40*, 102–114.

[2] Bojkovic, Z. S. Bakmaz, B. M. In addition, Bakmaz, M. R. (2008). Security Issues in Wireless Sensor Networks. *International journal of communications*, 2.

[3] Carman, D. W. Krus, P. S. and Matt, B. J. (2000) Constraints and approaches for distributed sensor network security. Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD.

[4] Chen, M. Gonzalez, S. Leung, V.C. (2007). Applications and design issues for mobile agents in wireless sensor networks. *IEEE Wireless Communication*, *14*, 20–6.

[5] Culler, D. E and Hong, W. (2004). Wireless Sensor Networks. *Communication of the ACM, 47*, 30-33.

[6] Douceur, J. (2002) the sybil attack. *International Workshop on Peer-to-Peer Systems* (IPTPS'02).

[7] Franklin, M. Galil, Z. and Yung, M. (2000). Eavesdropping games: a graph-theoretic approach to privacy in distributed systems," *J. ACM, 47*, 225–243.

[8] Karlof, C and Wagner, D. (2003). Secure routing in Wireless Sensor Networks: Attacks and Countermeasures, *Adhoc networks*, 293-395.

[9] Kurak, C and McHugh, J. (1992). A Cautionary Note on Image Downgrading in Computer Security Applications. *Proceedings of the eighth Computer Security Applications Conference*. 153-159.

[10] Murthy, C. R. In addition, Manoj, B. S. (2004). Transport layer and security protocols for ad hoc wireless networks. *Ad Hoc Wireless Networks - Architectures and Protocols*.

[11] Newsome, J. Shi, E. Song, D, and Perrig, A. (2004). The sybil attack in sensor networks: analysis & defenses. *Proc. of the third international symposium on Information processing in sensor networks*, 259 – 268.

[12] Parno, B. Perrig, A. and Gligor, V. (2005). Distributed detection of node replication attacks in sensor networks. In Proceedings of *IEEE Symposium on Security and Privacy*.

[13] Pathan, A S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S. (2006). A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks. *IEEE ICNEWS*.

[14] Perrig, A. Szewczyk, R. Tygar, J. D. Wen, V.and Culler, D. E. Spins: security protocols for sensor networks. *Wireless Networking, 8*, 521–534, 2002.

[15] Perrig, A. Szewczyk, R. Wen, V. Culler, D. and Tygar, J. D. (2002). SPINS Security Protocols for Sensor Networks, *Wireless Networks, eight*, 521-534.

[16] Perrig, A. Szewczyk, R. Wen, V. Culler, D. and Tygar, J. D. *SPINS: Security Protocols for Sensor Networks*. *International Conference on Mobile Computing and Networking* (MobiCom 2001).

[17] Priyanka, J. S. A. Tephillah, S. and Balamurugan, A. M. (2014). Attacks and countermeasures in WSN. *International Journal of Electronics & Communication*, *2*.

[18] Raymond, D. R. In addition, Midkiff, S. F. (2008). Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses, *IEEE Pervasive Computing*, *7*, 74-81.

[19] Rupinder Singh Brar, Harneet Arora. (2013). Mobile agent security issues in wireless sensor networks. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), 3*, 378-381.

[20] Saleh, M. and Khatib, I. A. (2005). Throughput Analysis of WEP Security in Ad Hoc Sensor Networks", Proc. *The Second International Conference on Innovations in Information Technology (IIT'05).*

[21] Santhi, G. Sowmiya, R. (2017). A Survey on Various Attacks and Countermeasures in Wireless Sensor Networks. *International Journal of Computer Applications, 159*, 0975 – 8887.

[22] Shi, E. In addition, Perrig, A. (2004). Designing secure sensor networks, *IEEE Wireless Communications, 11*, 38–43.

[23] Xu, W. Et al. (2005). The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. *Mobile Ad Hoc Net. In addition, Comp*. 46–57.

[24] Yu, Y. Li, K. Zhou, W and Li, P. (2011). Trust mechanisms in wireless sensor networks: attack analysis and countermeasures. *Journal of Network and Computer Applications, Elsevier*.