International Journal on Recent and Innovation Trends in Computing and Communication
Volume: 4 Issue: 12

ISSN: 2321-8169
288 – 293

# A Pragmatic Analysis on Diversified Aspects of Security and Integrity in Wireless Sensor Networks

Amit Sharma,
Asst. Professor,
School of Information Technology,
Apeejay Institute of Management Technical Campus,
Jalandhar, Punjab, India

**Abstract -** Wireless networks are susceptible and prone to assorted attacks at different layers from multiple sources and therefore it is required to understand the mechanism as well as taxonomy of attacks. By this perspective, there is need to investigate the network level attacks, their impact and remedial measures so that the overall scenario can be made secured. The nodes in wireless environment are affected adversely by number of attacks focusing of the resources used by the nodes participating in the communication. These network nodes are generally associated with the assorted functional aspects including battery or energy, power, log of neighboring nodes, cache and number of services. In a network attack, the malicious node or packet attempts to temporarily or permanently halt these parameters so that the authentic and realistic communication can be damaged. A number of algorithmic solutions work against assorted attacks but there is huge scope of research in this segment. This manuscript underlines the attacks on wireless networks with their related dimensions so that the effectual algorithm can be developed for overall security and integrity.

***Keywords**: Wireless Sensor Network, Reliable Communication, Wicked Wireless Node Attacks, Wireless Sensor Network Security*

*****

## 1. Introduction

In wireless networks, there are mobile nodes which are connected to each other using radio or related transmission line without any physical infrastructure. Wireless Network refers to a specific scenario having mobile nodes connected via mobile routers, base stations or satellites using which the overall network can be controlled and monitored. There are number of applications in which wireless sensor networks are integrated. In classical way, the wireless networks are implemented for the ease of mobility, remote accessibility and cross region connectivity.

### 1.1 Taxonomy of Wireless Technology Networks

- Wireless LAN
- Wireless WAN
- Wireless Mesh Network
- Wireless PAN
- Wireless MAN
- Cellular Network
- Global Area Network
- Space Network

### 1.2 Features of Wireless Networks

- Autonomous
- Dynamic and Effective Load Balancing
- Scalability
- Network Access Control
- Distributed, Arbitrary and Connected Operations
- Multihop based Routing
- Network Topology in Dynamic
- Network Scalability
- Light Weight Terminals
- Ease and Speed of deployment
- Decreasing dependency on infrastructure
- Mobility and Quality of Service
- Portability and Transportation

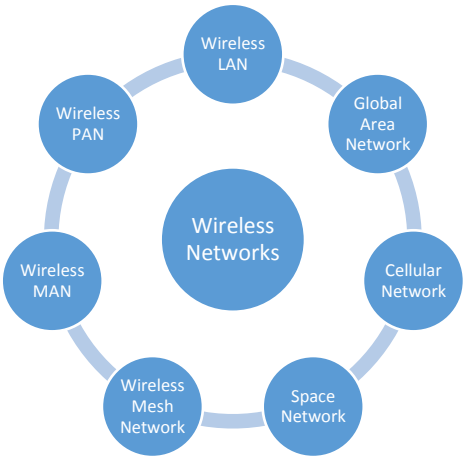


Figure 1: Wireless Networks and Associated Network Environments

ISSN: 2321-8169
288 – 293

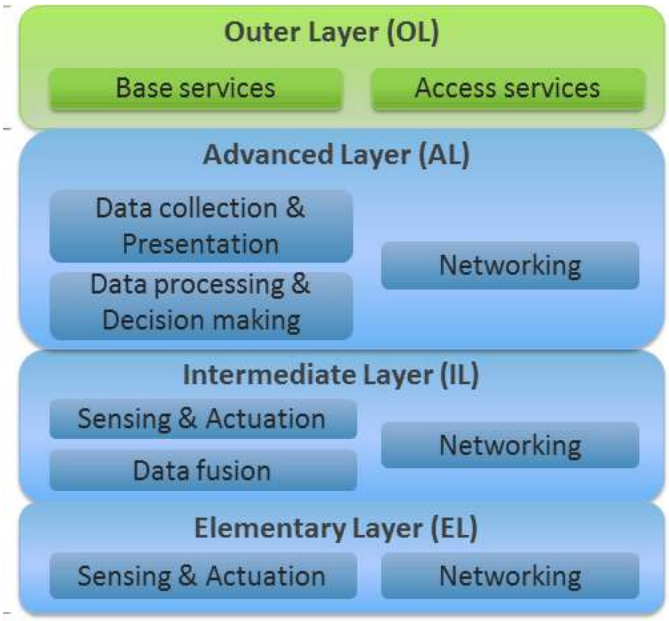


Figure 2: Layered Approach of Services and Aspects in Wireless Networks

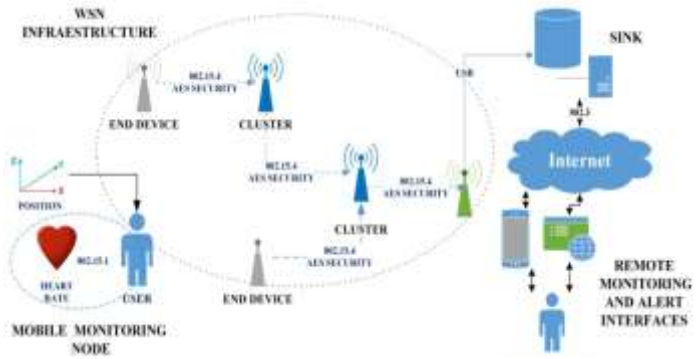


Figure 3: Traditional Scenario of Wireless Sensor Networks

The key attribute of a Wireless Network comprises

Source – Source Node (Mote)
CH – Cluster Head (Aggregator)
BS – Base Station (Tower)

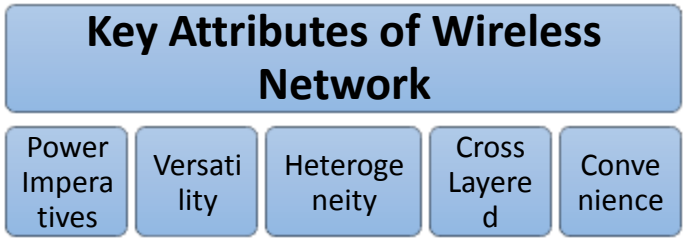


Figure 4: Key Attributes of Wireless Sensor Networks

Table 1 - Comparison Aspects of Wireless Networks Technology

| | Bluetooth | WiFi (a) | WiFi (b) | WiFi (g) | WiMAX |
|---|---|---|---|---|---|
| International Protocol and Standard | 802.15 | 802.11a | 802.11b | 802.11g | 802.16 |
| Frequency (In GHz) | 2.45 | 5 | 2.4 | 2.4 | 2 - 66 |
| Speed (In Mbps) | 0.72 | 54 | 11 | 54 | 80 |
| Range Parameter (meters) | 10 | 50 | 100 | 100 | 50 |
| Advantages | Low Cost | Speed | Low Cost | Speed | Speed, Range |
| Limitations | Range Issues | Cost Factor | Speed | Cost and Range both | Cost |

Each device or mobile node in a wireless scenario is having mobility and moves arbitrarily for data transmission with higher efficiency and integrity.

Table 2 – Comparison between WSN and Mobile Ad Hoc Networks

| WIRELESS SENSOR NETWORKS | MOBILE AD HOC NETWORKS |
|---|---|
| Energy Consumption more and generally non rechargeable due to remote and sensitive locations | Energy is not the issue because of recharging |
| Very far and not accessible physically in general | More close of Human Experts / Users |
| Data Aggregation / Grouping | No need of aggregation |
| Clustering | Each mobile node act as router itself |
| Security and Integrity are the key issues | Security is not an issue as it is always very close to human user |

**1.3 IEEE 802.11 Standards**

IEEE 802.11 refers to a set of specifications devised by IEEE for the representation of **w***ireless* **LAN** (WLAN) technology.

The standard 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. IEEE accepted this standard in year 1997.

**Table 3 - 802.11 Standards**

| Protocol / Standard | Classical Frequency (GHz) | Modulation |
|---|---|---|
| 802.11 (Wireless LAN) | 2.4 | DSSS, FHSS |
| 802.11 a (Wireless LAN) | 5 | OFDM |
| 802.11 b (Wireless LAN) | 2.4 | DSSS |
| 802.11 g (Wireless LAN) | 2.4 | OFDM |
| 802.11 n (MIMO with Additional Transmitter and Receiver) | 2.4/5 | MIMO-OFDM |
| 802.11 ac (MU-MIMO) | 5 | |
| 802.11 ad Under Development with higher transfer rate | 60 | OFDM, single carrier, low-power single carrier |
| 802.11 ah Wi-Fi HaLow | 1 | |
| 802.11 r Fast Basic Service Set, VoIP, Vo-WiFi | 5 | Voice Over WiFi, VoIP Roaming |

## 2. Security Threats in Wireless Networks

During the development of any system, the security and integrity is very important. It becomes mandatory to understand and evaluate the issues and factors which can affect the security directly or indirectly.

**Path Based Attacks -** These attacks are basic in remote wireless sensor systems. They are normally alluded as way based DoS (Denial of Service) attacks. Restricted hash chains can keep these attacks by constraining the rate at which hubs transmit parcels. In any case, one-way hash chains can't be utilized for a wide range of way based attacks. Particular techniques are utilized to wipe out particular sorts of path based attacks

**Rushing Attack -** Rushing attack occurs in on-interest directing conventions like DSR, Ad hoc On-Demand Distance Vector Routing (AODV) where course disclosure is finished by sending REQUEST messages to the neighboring hubs. In hurrying attack, the pernicious hub sends the REQUEST message much speedier when contrasted with the real hub. This outcomes in wrong course disclosure and the bundle is not sent to the destination. To keep this attack trust situated secured AODV convention is utilized where a trust edge worth is consolidated on the making trouble hub and in view of the trust esteem, the acting up hub can be detached. Another strategy is to utilize Rushing Attack Prevention (RAP) convention.

**Wormhole Attack -** In wormhole attack, the vindictive hub builds a passage (way) to the destination in such a path, to the point that all the bundles from the source are exchanged by means of the assailant which can change substance of the bundle before sending it to the destination. To keep this attack, packet confining system is utilized. A chain is data added to the packet in order to confine the packet path. A Packet rope is of two sorts: i) Geographical chain is in view of the separation and the position of the collector ii) Temporal rope is in light of the lifetime of the recipient.

**Routing Infrastructure Attacks -** Routing infrastructure concentrates on insignificant vitality steering, which intends to utilize negligible vitality to transmit and get parcels and by utilizing insignificant vitality ways to transmit bundles. However utilizing such plans may lessen the system network and lifetime of the system. To dodge such issues, a vitality mindful directing convention, which uses sub- ideal ways, was presented. Numerous steering ways are available where the convention picks one taking into account probabilistic qualities. For this situation, each steering way is given an opportunity to exchange bundles along these lines improving the system lifetime.

**Asset Exhaustion Attacks -** Resource consumption attacks concentrate on lessening the amount of assets utilized by hubs like battery force, stockpiling, memory and so forth therefore diminishing the general limit of the system. There are numerous sorts of attacks like merry go round attack, stretch attack, directional receiving wire attack, and malevolent revelation attack. Numerous systems, for example, free source steering, secure conventions or checking the way for any circles can be utilized to counteract such attacks. Numerous plans proposed in the writing manage the detection and/or avoidance from asset weariness attack for the most part limited to different levels of convention stack including Medium Access Control layer (MAC) and application layer. A next to no examination is done on the asset depleting attack steering layer.

The key threats to Wireless Technologies are hereby summarized

- **Interception or Eavesdropping** – Unauthentic access of the messages
- **Wormhole or False Gateway Attack –** Creating new or fake gateway for transmission of packets in non legitimate aspects. It refers to the creation of a new and fake hole or gateway from which the malicious packets can be transmitted
- **Non Optimal Path or Byzantine Allocation Attack –** Assignment of longest path rather than shortest to delay the network transmission.
- **Jamming** – Another type of Distributed Denial of Service attack in which the intruder distributes or access the network resources to non genuine dimension. It is considered as DDoS (Distributed Denial of Service) attack that choke the network path or complete channel to push back the genuine traffic
- **Blackhole attack –** In this attack the cracker modifies the data packets and fake channel is used for the delivery of signals. The intruder creates the cracking attempt for transmission of packets on fake or false channel
- **Byzantine attack –** Non optimal or simply long path is used by the attacker so that there is more overhead and higher delay in the transmission line
- **Rushing attack -** Creation of fake or false tunnel to overload the traffic from assorted dimensions. Two charmed aggressors use the tunnel philosophy to outline a wormhole. If a fast transmission way exists between the two terminations of the wormhole, the tunneled groups can multiply speedier than those through a standard multi-hop route.

### 2.1 Black Hole Attack

Black hole attack is the serious problem for the MANETs, in this problem a routing protocol has been used by malicious node reports itself stating that it will provides shortest path. In flooding based protocol, a fake route is created by the malicious node rather than the actual node, which results in loss of packets as well as denial of service (DoS).

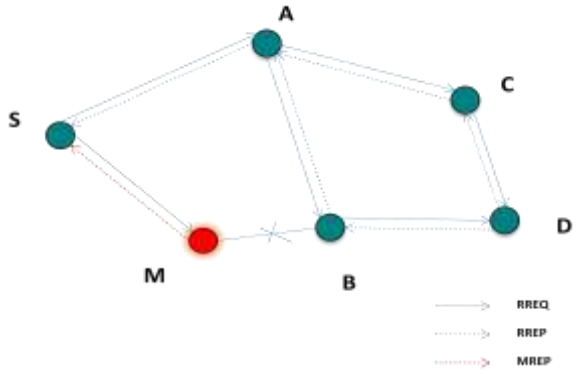


Figure 5: Black hole attack

In the fig 3, S and D nodes are the source and destination nodes, A B C are the intermediate nodes and M is the malicious node. RREQ and RREP are the key terms for route request and route reply respectively. MREP is abbreviation for malicious reply.

### 2.2 Two tier secure AODV (TTSAODV)

TTSAODV protocol is proposed earlier to prevent the black hole attack. In these protocol two levels of security is provided. During route discovery mechanism and data transfer mechanism. In this technique, black hole attack is easily identified either of these two techniques, even it fails in any of the mechanism. The major drawback in this technique causes enormous packet loss and delay in transferring packet. In the resource consumption attack, a malicious node can try to consume more battery life demanding too much of route discovery, or by passing unwanted packets to the source node. In the location disclosure based attack, the malicious node collects the information of routes map and then focus on further attacks. This is one of the unsolved security attacks against MANETs.

## 3. Related Works and Literature Review

There are a few difficulties posture by the asset constraints in the remote sensor arranges because of the vulnerabilities that may happen because of element conduct of systems. For deep and empirical analysis of the security and integrity aspects in wireless networks, a number of research papers are analyzed from various sources. Following are the approaches and conclusions of research papers and manuscripts.

[1] In this paper, a novel and effective approach for the energy encryption is addressed. The approach is associated with WPT (Wireless Power Transfer) for improving the overall performance of the network in terms of security and integrity. The proposed approach is uses dynamic, secured and authorization based energy consumption so that the overall performance of network can be enhanced.

[2] In this research manuscript, an effective and high performance approach for security in clustered wireless environment is proposed. This approach used is query process based paradigm to implement the security in wireless networks. Using the proposed approach in this paper, the security and integrity is preserved on multiple parameters against various attacks

[3] In this paper, the authors address the use and integration cryptographic hash approaches for implementation of security and authentication in wireless networks. This work underlines and implements MD5 (Message Digest) and SHA (Secured Hash Algorithm) as a hybrid algorithm to ensure and enhance the security in wireless networks

[4] In this work, the lightweight cryptography is implemented for security and privacy issues in the wireless networks. A unique and effective ultra lightweight approach KLEIN to improve the overall efficiency of the network environment is proposed and implemented.

[5] Homomorphic Encryption is the base issue taken in this work. In this paper, the authors implemented symmetric encryption and homomorphic encryption for performance evaluation. Finally, it is found and concluded that the performance cannot be highly improved using homomorphic encryption approaches

[6] In this paper, the authors propose a lightweight hash, Neeva-hash fulfilling the especially critical considered lightweight cryptography. Neeva-hash depends on upon wipe method for cycle with programming liberal change which gives excellent ability and required security in RFID progression. The proposed hash can be utilized for some application based purposes.

[7] The work in this paper addresses the issues of WSN requests and lightweight security. This paper addresses and devises a new approach for security and integrity in the wireless networks.

[8] This work considers two applications: “hop by hop transmission of information from cluster nodes to the base station and direct communication to clustered nodes information by mobile clients by strategy for mobile gadgets. Because of the hardware blocks of WSNs, some irrelevant effort operations, for occurrence, symmetric cryptographic approaches and hash functions points are utilized to finish a dynamic key association. The session key can be redesigned to keep dangers of assault from every correspondence. With these strategies, the information accumulated in wireless sensor networks can be all the more safely gave. Additionally, the proposed plan is dejected down and separated and related game plans”. In addition, a NS2 era is made in which the exploratory results demonstrate that the designed correspondence convention is workable.

[9] In this paper, the issue of key management is addressed for security and integrity in the wireless environment. The key goal of this research manuscript is to evaluate, compare and extract the suitable and high performance protocol for the wireless scenarios.

[10] To address the objectives of security and respectability, this paper proposes a lightweight module considering the robust operations. The proposed cryptographic game plan utilizes elliptic turn focuses to attest the going on focus focuses and as one of the puzzled helper parameters to make the pseudorandom bit movement. This social occasion is utilized as a bit of XOR, change and creamer operations with a specific completed target to encode the information pieces. The trial results in light of Mica2 sensor bit display that the proposed encryption game plan is nine times complex than the LED custom and two times speedier than the TWINE convention. The authors have also performed distinctive certain tests and cryptanalytic assaults to study the security way of the calculation and found the figure provably secure.

## 4. Conclusion and Scope of Future Work

There are number of algorithms and approaches for encryption and dynamic cryptography for security in wireless networks. Still, there is need to propose, devise and implement the salt based hybrid and dynamic cryptography so that the higher level of security and integrity can be proposed. The networks should be secured with the design of a new algorithm using hybrid cryptography approach for security in the wireless base control station. The current cryptography approaches can be made hybrid and high performance using metaheuristic approaches including Ant Colony Optimization, Simulated Annealing, Honeybee Algorithm, Firefly Algorithm, River Formation Dynamics and many others.

## References

[1] Aydos, M., Sunar, B., & Koc, C. K. (1998). An elliptic curve cryptography based authentication and key agreement protocol for wireless communication. In 2nd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications Symposium on Information Theory.

[2] Biswas, K., Muthukkumarasamy, V. and Singh, K., 2015. An Encryption Scheme Using Chaotic Map and Genetic Operations for Wireless Sensor Networks. Sensors Journal, IEEE, 15(5), pp.2801-2809.

[3] Bussi, K., Dey, D., Kumar, M. and Dass, B.K., 2016. Neeva: A Lightweight Hash Function.
[4] Carl Endorf, Eugene Schultz and Jim Mellander, Intrusion Detection & Prevention, McGraw-Hill, 2004
[5] Chen, C.L., Chen, C.C. and Li, D.K., 2015. Mobile Device Based Dynamic Key Management Protocols for Wireless Sensor Networks. Journal of Sensors, 2015.
[6] Cochavy, Baruch, Method of efficiently sending packets onto a network by eliminating an interrupt, US Patent Issued on August 18, 1998
[7] Dimitris M. Kyriazanos, Neeli R. Prasad, Charalampos Z. Patrikakis, A Security, Privacy and Trust Architecture for Wireless Sensor Networks, 50th International Symposium ELMAR-2008, 10-12 September 2008, Zadar, Croatia
[8] Donna Andert, Robin Wakefield, and Joel Weise, Professional Services Security Practice, Sun BluePrints™ OnLine - December 2002, Trust Modeling for Security Architecture Development
[9] Ghosal, A. and DasBit, S., 2015. A lightweight security scheme for query processing in clustered wireless sensor networks. Computers & Electrical Engineering, 41, pp.240-255.
[10] Kiruthika, B., Ezhilarasie, R. and Umamakeswari, A., 2015. Implementation of the Modified RC4 Algorithm for Wireless Networks. Indian Journal of Science and Technology, 8(S9), pp.198-206.