International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 02 | Feb -2017 www.irjet.net p-ISSN: 2395-0072

A Study of Safety Systems and Issues in Wireless Sensor Networks

Sunil B Somani[1], Dr.Athar Ali[2]

[1] *Ph.D. Research Scholar, Maharishi University of Information Technology, Lucknow, UP,India*
[2] *Research Guide, Maharishi University of Information Technology, Lucknow, UP, India*

Abstract - *Wireless Sensor networks (WSN) is a developing technology and have extraordinary potential to be utilized in basic circumstances like theaters of operations and business applications, for example, building, movement observation, environment observing and smart homes and numerous more situations. One of the major challenges wireless sensor networks face today is security. While the sending of sensor nodes in an unattended environment makes the networks defenseless to a mixture of potential attacks, the inalienable force and memory restrictions of sensor nodes makes routine security results unfeasible. The sensing technology joined together with preparing power and wireless communication makes it productive for being abused in incredible amount in future. The wireless communication technology likewise secures different sorts of security dangers. This paper examines a wide mixture of attacks in WSN and their characterization instruments and diverse securities accessible to handle them incorporating the tests confronted.*

Key Words*: *Security attack, Security system, Intrusion detection, Privacy

1. INTRODUCTION

Essentially, sensor networks are provision subordinate. Sensor networks are fundamentally intended for ongoing accumulation and dissection of low level data in antagonistic environments. Therefore they are generally suited to a significant measure of following and observation applications. Well known wireless sensor network applications incorporate natural life following, bushfire reaction, military order, shrewd communications, mechanical quality control, perception of discriminating foundations, smart edifices, conveyed mechanical technology, movement screening, looking at human heart rates and so forth. Larger part of the sensor network are sent in dangerous environments with animated wise resistance. Henceforth security is a pivotal issue.

One evident illustration is battleground applications where there is a pressing need for secrecy of area and imperviousness to subversion and demolition of the network. Less evident however exactly as vital security subordinate applications incorporate:

•Disasters: In numerous catastrophe situations, particularly those actuated by terrorist exercises, it may be important to secure the area of setbacks from unapproved divulgence

•Public Safety: In applications where concoction, living or other environmental dangers are screened, it is essential that the accessibility of the network is never undermined. Attacks initiating false cautions might lead to frenzy reactions or surprisingly more dreadful add up to carelessness for the signs.

•Home Healthcare: In such applications, privacy protection is crucial. Just commissioned clients ought to have the capacity to question and screen the network.

•The real commitment of this paper incorporates characterization of security attacks, security systems and challenges in Wireless Sensor Networks. Area 2 gives the point by point information about the security objectives in Wireless Sensor Networks. Security attacks and their characterization are talked over in area 3. Segment 4 talks over about the different security systems. Major tests confronted are given in Section 5 emulated by the conclusion area.

ATTACKS ON SENSOR NETWORKS

Wireless Sensor networks are susceptible to security attacks because of the broadcast nature of the transmission medium. Besides, wireless sensor networks have an additional defencelessness in light of the fact that nodes are regularly put in a threatening or unsafe environment where they are most certainly not physically ensured. Fundamentally attacks are considered dynamic attacks and latent attacks. Figure1 shows the characterization of attacks under general classifications and Figure 2 shows the attacks classification on WSN

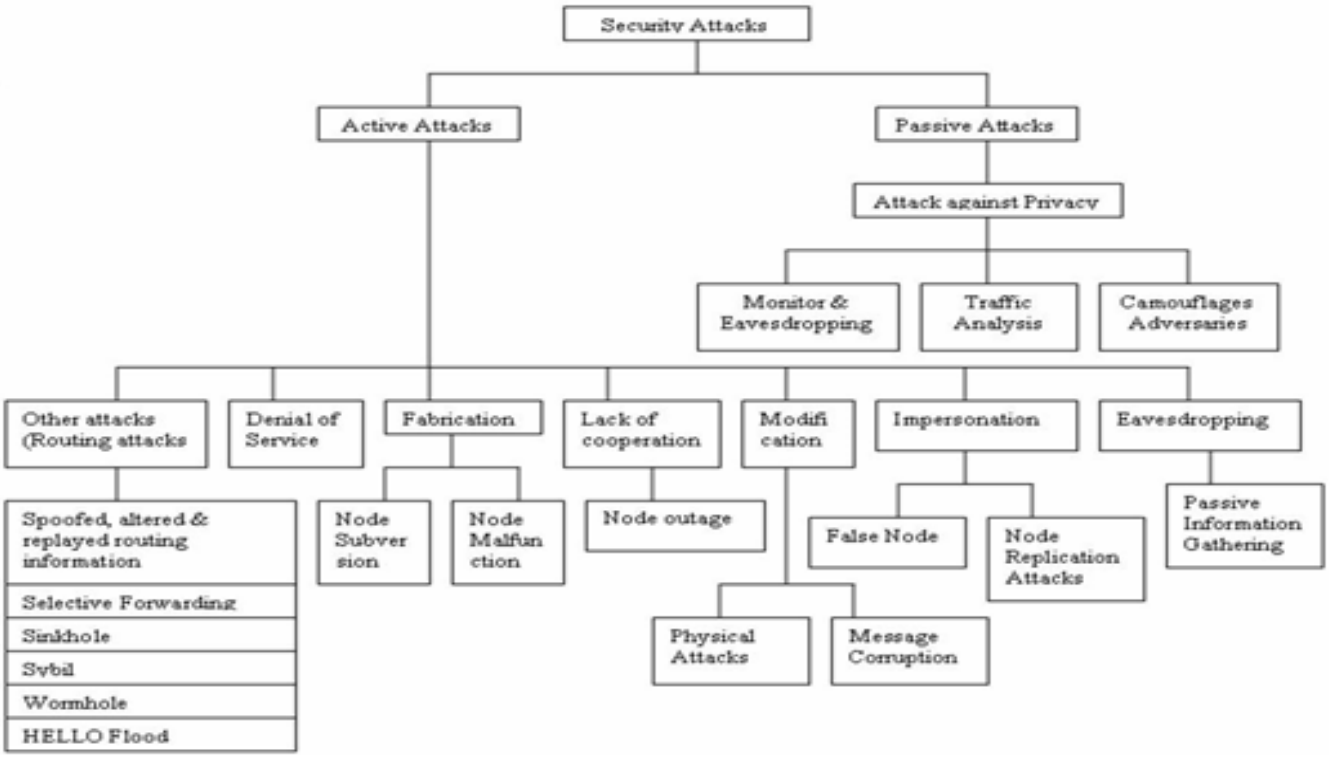

Figure 1. General Classification of Security attacks

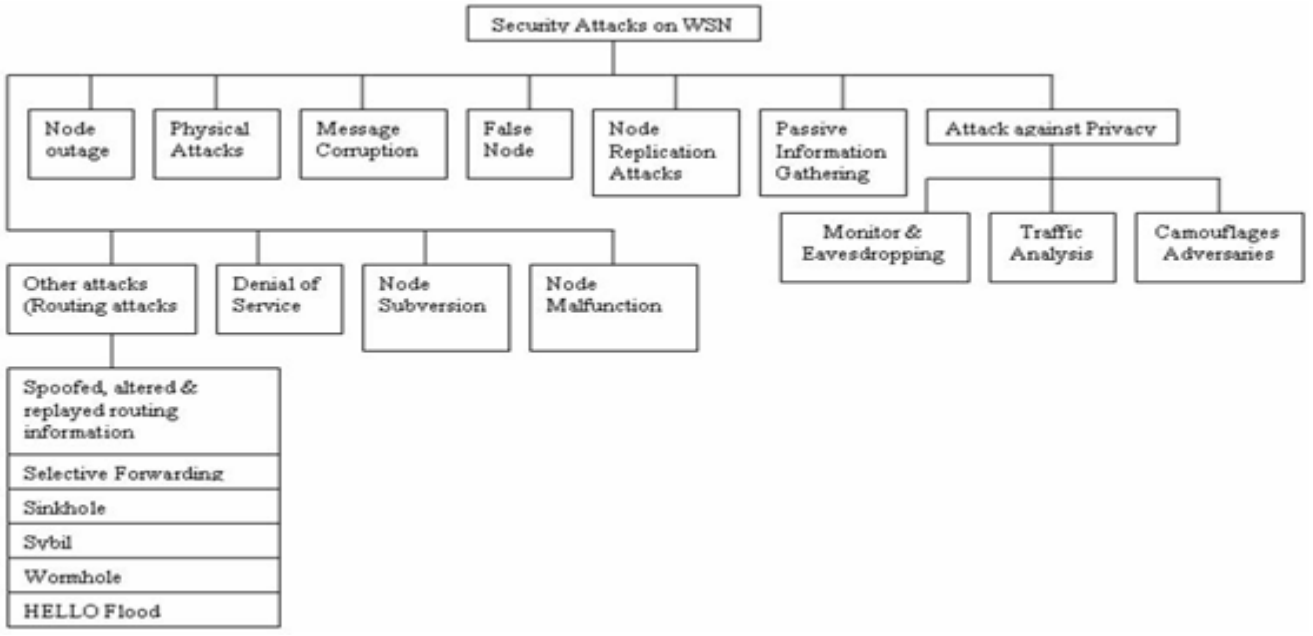

Figure 2. Classification of Security Attacks on WSN

The following and listening of the communication channel by unapproved ambushers are regarded as uninvolved ambush. The attacks against privacy is inactive in nature. The principle privacy issue is not that sensor networks empower the gathering of information. Indeed, much information from sensor networks could presumably be collected through immediate site observation. Rather, sensor networks escalate the privacy issue on the grounds that they make substantial volumes of information effectively accessible through remote access. Consequently, adversaries require not be physically present to uphold reconnaissance. The unapproved ambushers screens, listens to and changes the data stream in the communication channel are reputed to be dynamic assault.

SECURITY SYSTEM

The security instruments are really used to discover, avert and recoup from the security attacks. A wide mixture of security plans could be imagined to counter pernicious attacks and these could be ordered as high level what's more low-level. Figure 3 shows the request of security systems.

1. Key establishment and trust setup
2. Secrecy and authentication
3. Privacy
4. Robustness to communication denial of service
5. Secure routing
6. Resilience to node capture

1) *Key establishment and trust setup*- The primary requirement of setting up the sensor network is the establishment of cryptographic keys. Generally the sensor devices have limited computational power and the public key cryptographic primitives are too expensive to follow. Key-establishment techniques need to scale to networks with hundreds or thousands of nodes. In addition, the communication patterns of sensor networks differ from traditional networks; sensor nodes may need to set up keys with their neighbors and with data aggregation nodes. The disadvantage of this approach is that attackers who compromised sufficiently and many nodes could also reconstruct the complete key pool and break the scheme.

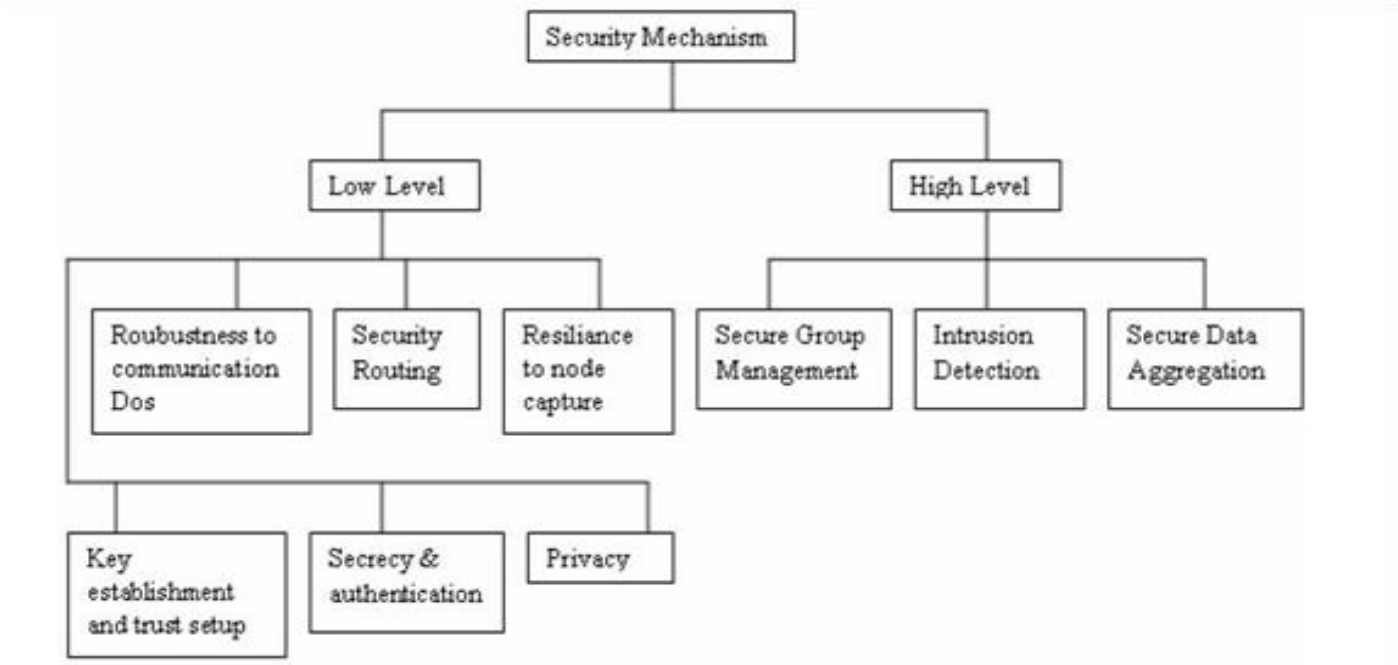

Figure3: Security mechanisms

2) *Secrecy and authentication* - Most of the sensor network applications require protection against a eavesdropping, injection, and modification of packets. Cryptography is the standard defense. Remarkable system arise when incorporating cryptography into sensor networks. Foe point-to- point communication Low-level security primitives for securing sensor Networks includes,

End-to end cryptography achieves a high level of security but requires that keys be set up among all end points and be incompatible with passive participation and local broadcast. Link layer cryptography with a network wide shared key simplifies key setup and supports passive participation and local broadcast, but intermediate nodes might eavesdrop or alter messages. The earliest sensor networks are likely to use link layer cryptography, because this approach provides the greatest ease of deployment among currently available network cryptographic approaches.

3) *Privacy*- Like other traditional networks, the sensor networks have also force privacy concerns. Initially the sensor networks are deployed for legitimate purpose might subsequently be used in unanticipated ways. Providing awareness of the presence of sensor nodes and data acquisition is particularly important.

4) *Robustness to communication denial of service* - An adversary attempts to disrupt the network's operation by broadcasting a high-energy signal. If the transmission is powerful enough, the entire system's communication could be jammed. More sophisticated attacks are also possible; the adversary might inhibit communication by violating the 802.11 medium access control (MAC) protocol by, say, transmitting while a neighbor is also transmitting or by continuously requesting channel access with a request-to send signal.

5) Secure routing - Routing and data forwarding is a crucial service for enabling communication in sensor networks. Unfortunately, current routing protocols suffer from many security vulnerabilities. For example, an attacker might launch denial of-service attacks on the routing protocol, preventing communication. The simplest attacks involve injecting malicious routing information into the network, resulting in routing inconsistencies. Simple authentication might guard against injection attacks, but some routing protocols are susceptible to replay by the attacker of legitimate routing messages.

6) *Resilience to node capture* - One of the most challenging issues in sensor networks is resiliency against node capture attacks. In most applications, sensor nodes are likely to be placed in locations easily accessible to attackers. Such exposure raises the possibility that an attacker might capture sensor nodes,

extract cryptographic secrets, modify their programming, or replace them with malicious nodes under the control of the attacker. Tamper-resistant packaging may be one defense, but it's expensive, since current technology does not provide a high level of security. Algorithmic solutions to the problem of node capture are preferable.

High-level security mechanisms for securing sensor networks, includes secure group management, intrusion detection, and secure data aggregation.

1) Secure group management - Each and every node in a wireless sensor network is limited in its computing and communication capabilities. However, interesting in-network data aggregation and analysis can be performed by groups of nodes. For example, a group of nodes might be responsible for jointly tracking a vehicle through the network. The actual nodes comprising the group may change continuously and quickly. Many other key services in wireless sensor networks are also performed by groups. Consequently, secure protocols for group management are required, securely admitting new group members and supporting secure group communication. The outcome of the group key computation is normally transmitted to a base station. The output must be authenticated to ensure it comes from a valid group.

2) Intrusion detection - Wireless sensor networks are susceptible to many forms of intrusion. Wireless sensor networks require a solution that is fully distributed and inexpensive in terms of communication, energy, and memory requirements. The use of secure groups may be a promising approach for decentralized intrusion detection.

3) *Secure data aggregation* - One advantage of a wireless sensor network is the finegrain sensing that large and dense sets of nodes can provide. The sensed values must be aggregated to avoid overwhelming amounts of traffic back to the base station. For example, the system may average the temperature of a geographic region, combine sensor values to compute the location and velocity of a moving object, or aggregate data to avoid false alarms in real-world event detection. Depending on the architecture of the wireless sensor network, aggregation may take place in many places in the network. All aggregation locations must be secured.

ISSUES OF SENSOR NETWORKS

The way of extensive, ad-hoc, wireless sensor networks presents huge challenges in planning security plans. A wireless sensor network is an exceptional network which has numerous demand contrasted with a traditional computer network.

A. Wireless Medium - The wireless medium is naturally less secure since its broadcast nature makes listening in straightforward. Any transmission can effortlessly be blocked, adjusted, or replayed by an adversary. The wireless medium permits an ambusher to effortlessly block quality bundles and effectively infuse pernicious ones. In spite of the fact that this issue is not unique to sensor networks, traditional results must be adapted to productively execute on sensor networks.

B. Ad-Hoc Deployment - The ad-hoc nature of sensor networks intends no structure might be statically characterized. The network topology is dependably subject to changes because of hub disappointment, addition, or mobility. Nodes may be sent via airdrop, so nothing is known of the topology before arrangement. Since nodes might fizzle or be reinstated the network must help self-arrangement. Security plots must have the ability to work inside this powerful environment.

C. Dangerous Environment - The following testing element is the antagonistic environment in which sensor nodes

capacity. Bits face the likelihood of devastation or catch by assailants. Since nodes may be in a dangerous environment, assailants can effortlessly pick up physical access to the devices. Agressors might catch a hub, physically dismantle it, and concentrate from it profitable information (e.g. cryptographic keys). The highly dangerous environment speaks to a genuine challenge for security specialists.

D. Resource Scarcity - The amazing resource confinements of sensor devices posture extensive tests to resource-ravenous security systems. The fittings requirements require to a great degree proficient security calculations as far as data transfer capacity, computational many-sided quality, and memory. This is no paltry undertaking. Vigor is the most valuable resource for sensor networks. Communication is particularly unreasonable as far as force. Unmistakably, security systems must give unique exertion to be communication proficient keeping in mind the end goal to be vigor effective.

E. Tremendous Scale - The proposed scale of sensor networks represents a critical challenge for security systems. Essentially networking tens to a huge number of nodes has turned out to be a considerable undertaking. Giving security over such a network is similarly testing. Security systems must be adaptable to extremely expansive networks while keeping up high reckoning furthermore communication proficiency.

CONCLUSIONS

The organization of sensor nodes in an unattended environment makes the networks defenseless. Wireless sensor networks are progressively being utilized as a part of military, environmental, health and business applications. Sensor networks are inalienably not quite the same as traditional wired networks and wireless ad-hoc networks. Security is an significant characteristic for the sending of Wireless Sensor Networks. This paper outlines the attacks and their orders in wireless sensor networks and likewise an endeavor has been made to investigate the security component broadly used to handle those attacks. The tests of Wireless Sensor Networks are additionally quickly examined. This overview will surely spur future analysts to come up with smarter and more strong security instruments and make their network more secure.

REFERENCES

[1] Adrian Perrig, John Stankovic and David Wagner,"Security in Wireless Sensor Networks"Communications of the ACM, Page53-57, 2004

[2] Al-Sakib Khan Pathan, Hyung-Woo Lee and Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", International conference on Advanced Computing Technologies, Page1043-1045, 2006

[3] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and countermeasures",AdHoc Networks (elsevier), Page: 299-302, 2003

[4]Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, 2002

[5] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, 2006

[6] Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication Technology (ICACT), Page(s):6, 2006

[7] Tahir Naeem and Kok-Keong Loo, "Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks", International Journal of Digital Content Technology and its Applications, Page 89-90 Volume 3, Number 1, 2009

[8]Undercoffer, J., Avancha, S., Joshi, A. and Pinkston, J. "Security for sensor networks". In Proceedings of the CADIP Research Symposium, University of Maryland, Baltimore County, USA, 2002

[9] Zia, T.; Zomaya, A., "Security Issues in Wireless Sensor Networks", Systems and Networks Communications (ICSNC) Page(s):40 – 40, 2006

[10] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, "Sensor Network Security: A Survey", IEEE Communications Surveys & Tutorials, vol. 11, no. 2,page(s): 52-62, 2009

[11] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, pp. 30-33,2004

[12] D. Djenouri, L. Khelladi, and N. Badache, "A Survey of Security Issues in Mobile ad hoc and Sensor Networks," IEEE Commun. Surveys Tutorials, vol. 7, pp. 2–28, 2005.

[13] S. Schmidt, H. Krahn, S. Fischer, and D. Watjen, "A Security Architecture for Mobile Wireless Sensor Networks," in Proc. 1st European Workshop Security Ad-Hoc Sensor Networks (ESAS), 2004.

[14] Y. Wang, G. Attebury and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Commun. Surveys Tutorials, vol. 8, pp. 2–23, 2006.

[15] Yun Zhou, Yuguang Fang, and Yanchao Zhang, "Securing Wireless Sensor Networks: A Survey", IEEE Communications Surveys & Tutorials, 2008