Analysis of Security Requirements, Attacks and Vulnerabilities at Transport Layer in Wireless Sensor Networks

Sunil Ghildiyal
Uttaranchal University
Dehradun Uttarakhand

Anupam Semwal
Drona College of Mgmt. & Tech. Ed.
Dehradun Uttarakhand

Jainendra Singh Rana
Uttaranchal University
Dehradun Uttarakhand

ABSTRACT
For about last two decades research and development processes in area of Electronics and Sensors have resulted as significant advancements in electronics and technology, small size, cost effectiveness have resulted sensor nodes as crucial part of real world problem solution applications. The wireless sensor nodes are spread over an area to record the facts of situations like fire, flood and then forward same to meaningful data to the a node, which is generally cluster head node for calculations, resulting an alert to take necessary measures to control the situation. In last few years, WSN have increased significantly in variety of areas and applications, resulted the contemporary demand of high, consistent security mechanism. Also, there is variety of attacks on WSN at their different layers. These tiny, low processing sensor nodes are not strong enough in terms of power, handling attack issues etc. On other hand, applications based on these sensors demand on-time streamed data or information is to be collected and then to send same on a reliable, secure delivery mechanism. Tiny sensors with limited hardware, processing are not able to afford old and in practice security protocols or algorithms to face or sustain the attacks. Many attacks impact WSNs. at their different layers an affect sensor's roles like signaling, framing, transmission etc. Many attacks have been identified at each layer of WSN which are intended, pre-planned attacks to obstacle the availability of service, restricting the sensor node's utilization in solution of a for problem. This paper is mainly focused on WSN structure, threats, attacks and security requirements and security measures against attacks; especially various types of attacks starting from physical layer and data link, network layers, subsequently and particularly variety of attacks at transport layer in details with some effective suggestions as prevention or protection against those attacks.

Keywords
Wireless, Sensor, Security, Processing, Attack, Bandwidth, Vulnerabilities, Networks

1. INTRODUCTION
As a result of recent developments in wireless technology polishing, wireless networks are now believed as a reliable architecture medium to deliver communication with major security parameters confidentiality, integrity and availability and non-repudiation. Wireless Sensor Networks consist of less power, less processing capability, small size nodes[1]. Hence, It becomes very tough to raise the capability level of such tiny sensors due to their various constraints. Constraints, associates with sensors are to be considered seriously while designing a secure real world problem solution using WSN.

Actually, sensor nodes use RF for messaging, communication and hence use broadcast basically. Since medium is open, it is tedious to protect the broadcast from easy eavesdropping, as injecting can be done very easily over wireless broadcasting. Also, sensor nodes are scattered over an geographical area in physically insecure pattern, can be stolen easily, can be tempered physically or replayed or reprogrammed after capturing. Insecure, open deployment of sensor nodes make them to be easily detected for intended damage[2]. These low and limited power capacity nodes make WSNs. very weak and paralyzed architecture in front of any intended attack like flooding or replaying etc. One of the initial measure against these threats may be authorization access checklist available with them to detect unauthorized or malicious users, which may harm the entire node or network.

2. REVIEW OF LITERATURE
There is diversity in the set of challenges in sensor networks and primarily focused on supporting multi-hop communication, data management, geographic routing challenges in networks Ganeshan et al.[3]

Recent surveys and forecast predict that there is going to be increase in the number of wireless devices including phones, mobile devices tremendously. These are generally computers of all kinds, notebooks, and sensor nodes that forming internet scenario Horst Hellbruck et al.[4]

In last two decades, developments in electronic mechanical sensors have made application domains diverse due to availability of variety of tiny micro sensors which consists with low power wireless communications. These can be very densely deployed with their self configuration and management features in different areas solving real world problems Kalitha et al.[5].

These wireless sensors are not isolated from attacks easily. They are very much prone to physical attacks and tempering. Any traditional security algorithm can also not be applied on these due to low power and processing resource constraint Kavitha et al.[6]

3. WSN CHARACTERISTICS
For last about two decades, WSNs. have received a lot of interest by the researchers, industry. This is cause of those to be less cost solutions to many real world problem solving applications. Other favoring factors are easy to use, low energy consuming nodes, portability, unattended operation even in no men land with an ability to withstand bad

geographical, environmental situations, having dynamic network topology as per situation, faster recovery methods or alternates with sensor node stopping and failures, Mobility of nodes, Heterogeneity of nodes and at all highly scalable in terms of topology and deployment.

4. WSN CONSTRAINTS

Resource: Tiny sensors are equipped with low processing capability processors and a low RF linking bandwidth capacity. It is by virtue of small hardware size and very small battery for power backup. Hence, computational capabilities are also affected by these constraints tremendously in WSNs.

Memory: Though sensor nodes consist of a flash memory and flash RAM, but loading of OS and other system applications and utilities consume much memory space, which result in remaining very less space for other application tasks and any storage. In sensor nodes, flash memory is used for storing downloaded application code too.

Self-Organization: A wireless sensor network is a ad hoc network, where every sensor node has to be independent and flexible enough for self-organization and self-healing under various conditions. WSNs. are designed for forming random infrastructure as per condition and subsequently also need network management in a sensor network by nodes themselves primarily.

Message size: If we compare to any existing traditional network, WSNs. consist messages of very small size which subsequently result in no concept of segmentation in applications usually.

Ad-Hoc Deployment over Wireless Medium in Hostile Environment: Due to broadcast nature, wireless channel is less secure and makes eavesdropping easy. The wireless channel carrying information can easily be intercepted and then altered or replayed. But there are traditional solutions which can be adapted by WSNs. for efficient execution [7]. Ad-hoc nature of sensor networks defined no static structure. The network topology is changed frequently due to node failure, node addition or node mobility. In WSNs. nodes may fail and get replaced in the network, must have self-configuration and self-organization. In hostile environment, nodes or motes face problem of capturing and possibility of destruction. Due to it, attackers may capture a node, and can physically disassemble the node.

Unreliable Communication and Unattended Operation: In WSNs., Generally routing of the sensor network is connectionless and unreliable for data transfer[8]. In addition, There may be Conflicts due to broadcasting. The multi-hop routing and bandwidth congestion may lead to latency. It results in loss of synchronization among sensor nodes In many conditions, sensor nodes may be left in open unattended environment for a long time. It leads to exposure to physical attacks directly. Also it requires remote management of the nodes in absence of central management point. Absence of central management results in improper operation of network or network malfunctioning.

Node Location: Generally, nodes are very small and scattered in an large open area. Very frequent dislocation of nodes by disaster conditions like earthquake or avalanche or power winds etc. can occur. Mobility of nodes may also result in locating the nodes tough. This location instability affects data, collected by the nodes after they have been deployed at specific place or have been or not constant static at same place for a specific time period.

Absence of global addressing: In typical WSN real world applications, nodes are scattered over a geographical area in large quantity even hundreds or thousands. This huge amount of sensors results as generally no identification of nodes and also as impossibility of providing unique addressing at global level.

Redundant Data: Very high chance of data redundancy are observed as multiple nodes may capture the same data of same incident.

Data Availability: Whatever date acquired by nodes must be available for use of the resources of network and also there will always be network available with the messages to communicate with further infrastructure. In WSN, failure of BS or group or cluster head's availability will also lead to threaten to the functioning of the entire sensor network. Hence it is recommended to implement, maintain and tune a proper operational network.

5. WSN SECURITY REQUIREMENTS

The main aim of security architecture is to preserve the data contents from various vulnerabilities and attacks. Security measures has to ensure that services would be available in presence of any attacks even in case of DoS attacks also or any other serious vulnerability. It will make sure that only one authorized node can be a part of information propagation. It results as a malicious node to be failure to masquerade as trusted node. Also there is a high demand of having confidentiality maintained with data integrity when authorized users or nodes are transmitting, receiving or forwarding the information, Data freshness and non-repudiation are also other factors to be considered as main parameters of security mechanisms. WSN nodes are light weight and generally deployed randomly, operated even in unattended environment subsequently in a non-physically secured environment. They rigorously present the security architecture by their own intuitions including self-organization of node which generally refers self-configuration, autonomous self-management and self-healing.

6. DEFENCE COMPLICATIONS IN WSN

Planning and implementing security in WSN is complicated by the own various constraints and capabilities limitations. Nodes are susceptible to physical Capture. Nodes use wireless channel, which is easy to eavesdropping. Attacker can easily inject malicious codes into the network Anti-jamming techniques such as FHSS and temper proof nodes are rarely possible in a sensor network. Small size, low cost, and limited power make WSNs more susceptible to DoS attacks. Dynamic Ad-hoc topology of WSN Provides different types of link and connections to attackers for network penetrations. A single node can be compromised to destruct whole network operation. Large scale deployment of sensors itself demands huge security mechanisms. WSNs can be secured by compromising the minimal resource consumption and maximization of security technique levels. Asymmetric cryptography can also not be applied over sensor networks due to its expensiveness. Managing keys, and symmetric key cryptography are also expensive in terms of resource consumption and exhaustion. These all are restricted by architectural constraints like low memory, power and processing.

7. THREAT MODEL

In Wireless Sensor Networks, threats are from outside the network as well as within the network. Attacks are from nodes of the native network is much harmful. Also, it becomes quite difficult to find out the malicious or compromising node within the native network. Attacks may be classified as passive and active attacks where passive attackers don't modify or alter the data as the active attackers do. Monitor and Eavesdropping, Traffic Analysis and Camouflage Adversaries are such category attacks where information is gathered by attacker but not altered or changed. Another classification is mote class attack where opponent attack is done by using similar capacity nodes for network penetration. Also in some cases, powerful devices like laptop are used to penetrate the network then such attack is called laptop attack.

8. WSN ATTACKS

Generally, WSN attacks can be divided into two major categories: invasive and non-invasive. Non-invasive attacks generally target to basic properties of signaling like timings, power and frequency of channel and trying to destroy core transmitting signaling system. However invasive type attacks aim to hamper the application malfunctioning, network routing failure and transport reliability failure which may further include availability of service, information transition, routing etc. One major variety of attack is DoS attack which aims the system to be totally inaccessible by flooding the channel generally. Many other common attacks are encountered during the transit of information. WSNs. may face attacks affecting the routing schemes, routing tables and routing algorithms mostly in general. Intended attacks of opponent are to destroy the entire network components or operations. Attacks may occur at every layer of OSI layers of WSN. Generally, Attacks penetrate the efficiency of aimed networks by affecting its associated protocols. Attacks may consume or exhaust the resources, alter the infrastructure configuration and can demolish the network components either partial or full. Wood and Stankovic presented layer wise categorization of attacks first [9], which was further enhanced by Raymond and Midkiff with some addendums [10].

Starting from physical layer, Jamming is one of attack at physical layer, in which RF used by the network nodes are interfered or adversary can either disrupt entire network which depends on the power of jamming nodes. There are variety of such attack like Deceptive, Random and Reactive [11]. One more attack at physical layer is tempering, in which attacker may physically temper the nodes and can compromise with them. At link layer exhaustion or continuous channel access is one of major attack where attacker may disrupt the channel by frequently requesting and transmission over it. Unfairness is also one of attack at which is referred as repeated collision based attack.

9. ATTACKS AT TRANSPORT LAYER

Ultimate goal of Transport Layer is to establish communication for extranets or WSN having connectivity with the internet. It is itself a challenging issue in wireless sensor networks. Interconnectivity with internet makes attacker to be so strong enough to easy access to the transport layer, due to the undetected at the previous layers. Transport layer attacks are injection of false messages and energy drain attacks and others as follows:

9.1.Flooding

A stateful protocol maintaining states many times faces a problem called flooding[12]. Attacker may repetitively fire flood such as new connection requests, to the network resources until those are completely exhausted, which could be needed by separate connections or have reached maximum limit. By virtue of it, further legitimate requests will be ignored, resulting a kind of non availability of resources to users. Prevention from flooding is most crucial task as it may exhaust resources rapidly.

One of suggestion to overcome this problem is to limit the number on concurrent connections over a session on a particular channel. This restriction on the number of connections prevents from complete resource exhaustion or channel exhaustion will be minor or negligible also in some case. The one of best way to prevent from such attack is by encouraging each connecting client to demonstrate its authorized valid commitment to the connection by puzzle solving.

9.2. De-Synchronization

This attack is also one more variety of intended attack. Connection between two endpoints can be disrupted by de-synchronization. In this attack, the attacker repeatedly forges messages to either or both endpoints. For example, one node may get multiple even fake requests for retransmissions of missed frames by the repeated spoof messages. If such requests are timed correctly, an attacker may degrade the functionality, capability of end hosts by retransmission of frames unnecessarily, somehow also consuming total channel bandwidth also. It results in endpoints to waste the energy for recovering from errors which never really exists particularly where nodes are already starving for energy. One possible solution to this problem is authentication of all packets exchanged, even all control fields in the transport protocol header. Many vendors have provided many algorithms, designed to overcome this attack.

9.3. Data Integrity Attack

Such attacks targets or make data compromised while data travelling among the nodes in WSN by either changing the data contents within the packets or injecting false data. But most noticeable is that attacker node must be much capable with more processing, memory and power than ordinary sensor nodes. The aim of this attack is to falsify sensor data. It also falsifies routing data in order to disrupt the sensor network's normal routing operation, possibly making it of no use. This is considered to be a type of DoS attack and can be defended by adapting asymmetric key encryption algorithm or system or digital signatures can be used in lieu of. But it adds lot of additional overhead to the resources constraint nodes.

9.4. Energy Drain Attack

WSN is low powered and dynamically arranged. It is difficult or impossible to replace/recharge sensor node batteries in solutions. It is due to limited amount of energy available and attackers may utilize compromised nodes to inject manipulated reports into the network or can generate large amount of traffic in the network.

These manipulated reports will lead false alarms to waste real world response efforts, and drain significant amount of power or energy in a battery based network. This attack is possible only if the intruder's node has enough energy to transmit packets at a constant rate. The goal of this attack is to destroy the sensor nodes in the network, bring down the performance

of the network and ultimately splitting the network grid. It may further results in introducing a new Sink node to taking over control [13].

10. CONCLUSION

There are various attacks to hamper the smooth functioning of wireless sensor networks like denial of sleep, homing etc. In many situations, attacks may overlap also with each other. It is difficult to measure the attacks and their solution at physical layer as sensors have native radios of very low power and are operated in open area, unattended environment, hence are very poor to resist such attacks. Though there are algorithms and security mechanisms for network security and protection from above attacks but cannot be applied in WSN nodes due to node's constraints. There is need of tiny low computational algorithms for WSN. However there are many algorithms existing for WSN infrastructure and being applied also. But those are failure to be proved as correct and fruitful measures against above attacks. DoS situation at any layer in WSN requires to be addressed by strong mechanism. It is recommended to develop a prevention scheme against attacks which can be applied already to make WSNs. much stronger against DoS attacks. DoS may appear as individual and sometime altogether. It is always advisable to develop and deploy a proper suitable measure in WSN as prevention already.

11. REFERENCES

[1] D. K. Chaitanya "Analysis of DoS attacks on WSN using simulation" Middlesex University.

[2] Ritu Sharma et. al. "Analysis of security protocols in wireless sensor networks" Int. Journal Advanced Networking and Applications Vol 02, Issue 03.

[3] Deepak Ganesan et al. " Parallel and Distributed Computing issues in WSN", Journal of Parallel and Distri.Computing, Volume 64, Issue 7, July 2004

[4] Horst Hellbruck, Max Pagely, Alexander Krollery "Using and Operating Wireless Sensor Network Testbeds with WISEBED" 2011 The 10th.IFIP Annual Mediterranean Ad hoc Networking Workshop

[5] Hemanta Kumar kalitha and Avijit Kar "Wireless Sensor Network Security Analysis" IJNGN Vol 1, Dec 2009

[6] T. Kavitha, D. Sridharan "Security Vulnerabilities in wireless Sensor Networks" IJAS 5 (2010) 031-44

[7] Tahir Naeem et.al. 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, year 2009.

[8] John Paul Walters et. al. "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006

[9] Wood, A. D. and Stankovic, J.A. (2002) " Denial of Service in Sensor Networks" IEEE Computer, vol. 35, no. 10, 2002, pp 54–62.

[10] Raymond, D. R. and Midkiff, S. F. (2008) "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses" IEEE Pervasive Computing, January-March 2008, pp 74-81.

[11] Xu, W., Trappe, W., Zhang, Y., and Wood, T. "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks' ACM MobiHoc'05, May 25–27, 2005, Urbana-Champaign, Illinois, USA, pp 46-57.

[12] Anthony D. Wood, John A. Stankovic " Denial of Service in Sensor networks" University of Virginia 0018-9162/02/$17.00 ©2002 IEEE

[13] Prabhudutta mohanty, Sangram Panigrahi, Nityananda sarma and siddhartha sankar satapathy "Security issues in WSN: a survey" Int. Journal of Theoretical and Applied Information Technology.