ANALYSIS OF WIRELESS SENSOR NETWORKS: SECURITY, ATTACKS AND CHALLENGES

Sunil Ghildiyal[1], Ashish Gupta[2], Musheer Vaqur[3], Anupam Semwal[4]

[1]*Assistant Professor, Department of CSE, Uttaranchal University, Prem Nagar, Dehradun (UK) India*
[2]*Assistant Professor, Department of IT, Dev Bhoomi Institute of Technology, Dehradun (UK) India*
[3]*Assistant Professor, Department of IT, Uttaranchal University, Prem Nagar, Dehradun (UK) India*
[4]*Assistant Professor, Department of Mathematics, IEC University, Alal Nagar, Baddi, Solan (HP) India*

Abstract

Recent advancements in MEMS technologies and development in the area of low power microcontrollers have resulted as implementation of wireless sensor networks in real life problem solving in areas like traffic monitoring, patient monitoring , battlefield surveillance. These wireless sensors are very small in size and are operated at low power for low data rate applications. WSN nodes include features like scalability, self-organizing, self-healing. WSN nodes face many challenges starting from deployment till their life span which is dependent on very low battery strength. Since these nodes are operated in unattended environments, many security threats are for them to survive. These nodes face variety of attacks at different layers of their architecture, ranging from physical stealing, tempering to reprogramming. Applying any traditional security mechanism over wireless sensor nodes is also not possible as those traditional algorithms or protocols consume very much processing and power due to their complexity. In this paper, we have mentioned. This paper aims at reporting an initial introduction of WSN, WSN architecture, challenges and security threats subsequently.

Keywords: *Wireless, Sensor, Threat, Security, Power, Node*

---***---

1. INTRODUCTION

Wireless Sensor networks (WSN) is an emerging technology that shows result oriented promise for many applications for defense as well as mass public[1].WSN nodes are low power, low cost smart devices having limited computing resources[2]. In last few recent years, Wireless Sensor Networks (WSNs) have gained worldwide attention particularly with the proliferation in Micro-Electro-Mechanical Systems (MEMS) technology which has facilitated the development of sensors[3]. Rapid demand of wireless sensor nodes indicates how these can be utilized in different areas of real-life applications. Main aim is to interpret, observe and handle the WSN node data at base station (BS). WSNs form an ad-hoc network that operate with nominal or no infrastructure. WSNs merge a wide range of information technology that spans multiple computer hardware vendors, software, networking and programming methodologies. WSNs make it possible to perceive what takes place in the physical world in ways, was not previously possible [4].

2. REVIEW OF LITERATURE

Set of challenges in sensor networks are diverse and focused on supporting multi-hop communication, data management, geographic routing challenges in networks and monitoring and maintenance of such dynamic, resource-limited WSNs. Ganeshan et al.[5] Current surveys and forecast predict that the number of wireless devices is going to increase tremendously. These wireless devices can be computers of all kinds, notebooks, net-books, Smart-phones and sensor nodes that evolve into real- world scenarios forming a ”Real-World-Internet” in the future. Horst Hellbruck et al.[6] In WSNs. application domains are diverse due to availability of tiny micro sensors with low power wireless communications. These can be densely deployed with their auto configuration features in different areas of application to solve real world problems. Kalitha et al.[7]. Wireless sensors are not isolated from attacks easily. They are prone to physical attacks. Any traditional security algorithm is not applicable due to resource constraint. Kavitha et al.[8]

3. CHARACTERISTICS OF WSN

The main characteristics of a WSN include: WSN are getting a lot of popularity day by day due to their low costing solutions to variety of real world applications, many other favoring factors of WSN use are low power consumption constraints for nodes: portability, unattended operation, using batteries or energy harvesting, ability to withstand bad environmental conditions, having dynamic network topology, to cope with node malfunctioning and failures, Mobility of deployed nodes, Heterogeneity of nodes, Scalability, at the time of deployment and after deployment, Easy use.

4. THREAT MODEL

In WSN, threats are from outside the network and within the network. If attacks are from the nodes of the native network then it is much harmful. Also, it is quite difficult to find out the malicious or compromising node within the native network. Another classification of the attacks may be passive and active where passive attacks don't modify or alter the data as active attacks do. If the opponent attack by using similar capacity nodes for network penetration it is called mote class attack but when powerful devices like laptop are used to penetrate the network then such attack is called laptop attack.

5. WSN SECURITY GOALS

Traditional security goals for an ad-hoc network and specific to the WSN security goals can be classifies in two categories as primary and secondary [9]. The primary goals are known as standard security goals such as Confidentiality, Integrity, Authentication and Availability (CIAA). The secondary goals are Data Freshness, Self-Organization, Time Synchronization and Secure Localization.

5.1 Primary Goals:

5.1.1 Data Confidentiality

Confidentiality means to reveal the data to the authorized persons only not to everyone in the networks. It is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential.

5.1.2 Data Integrity

It ensures the data during transition is not altered, tempered by an unauthorized one may be an attacker. Even if the network has confidentiality measures, there is still a possibility that the data integrity has been compromised by alterations. If any malicious node is present in the network or medium of transmission is damages, then also integrity may get affected [10].

5.1.3 Data Authentication

Authentication ensures the reliability of the message by identifying its origin. In WSN attacks, adversaries can also inject additional false packets [11]. Data authentication verifies the identity of the senders and receivers.

5.1.4 Data Availability

It is the ability of a node to ensure the availability of the resources for use. It also ensures the network for message communications. This goal of security ensures the functionality of the network. However failure of central hub or cluster head may make a node unavailable for use.

5.2 Secondary Goals:

5.2.1 Data Freshness

It ensures that data contents are recent and there no replay of any old content. Even though Integrity and confidentiality is there, data freshness is to be checked separately.

5.2.2 Self-Organization

Each node must be self organized, self configured while joining its ad-hoc nature networking environment. Nodes must be independent and must have self-healing capabilities even in critical situations. There is no any fixed infrastructure for WSN implementation, so nodes must their selves adapt the topology and deployment strategy.

5.2.3 Time Synchronization

Many WSN applications demand some form of time synchronization for execution. Sensors organized in group collaboration may require time synchronization for application tracking.

5.2.4 Secure Localization

Sensors may get displaced while deploying them or after a time interval or even after some critical displacement incident. The utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will require precise location in order to detecting fault location.

6. ATTACKS ON SENSOR NETWORKS

Broadcast nature of communication is WSN is vulnerability for them. Subsequently, wireless sensor networks have an additional threat from their physical deployment as these nodes are not physically protected. Mainly, attacks are classified as active attacks and passive attacks. All the classical techniques of attacks will also be applied on WSN. But due to limited capability of node, some specific attacks can also damage node and network subsequently. For examples an adversary can eavesdrop on the communication, perform traffic analysis of the observed network behavior, can replay the communication traffic later on. [12].

The attacks of WSN can be classified into two categories: invasive and non-invasive. Non-invasive attacks generally target to timings, power and frequency of channel. Invasive attacks target to availability of service, transit of information, routing etc. In DoS attack, hacker tries to make service or system inaccessible.

6.1 Attacks at Physical Layer

6.1.1 Jamming

Jamming attacks leads to the interference by identical radio frequencies used by the network nodes. The adversary can either disrupt entire network or a particular small portion of it. It depends on the power of jamming nodes distributed nearby the network. Jamming is of various types Constant, Deceptive, Random and Reactive[13]. Handling the jamming at MAC layer needs to control the requests which may exhaust the resources by ignoring them. However network layer also deals with jamming by mapping jamming area in the network or in surrounding routing area.

6.1.2 Tempering

As nodes are operated in unattended areas, attacker may physically temper the node and can compromise with them. It is not possible to control hundreds of nodes spread over large area. Attacker may extract the sensitive information like cryptographic keys from node by damaging it.

6.2 Attacks at Link Layer

6.2.1 Exhaustion (Continuous Channel Access)

In this attack, attacker may disrupt the channel by continuously requesting and transmitting over it. It results in starvation for channel access for other nodes. It is usually done by sending a large numbers of RTS (Request to Send) packets over channel, leading multiple collisions and draining out the nodes of their power.

6.2.2 Collision

Collision occurs when two nodes intend for simultaneous transmission on same frequency channel. If the packets collide, a small change in packet will take place which will be encountered as mismatch at the time of checksum at receiving end and hence packets will be discarded, to be re transmitted.

6.2.3 Unfairness

Unfairness is referred as repeated collision based or exhaustion based attacks or an abusive use of cooperative MAC layer priority mechanisms. Also may be called as a weaker form of DoS. This threat may not entirely prevent legitimate access to the access channel but it could degrade service in order to gain an advantage such as causing other nodes in a real-time MAC protocol to miss their transmission deadline.

6.3 Attack s at Network Layer

6.3.1 False Routing or Spoofed, Altered, Replayed Routing Information

Such attacks primarily focus on routing protocols mainly for routing information. While nodes exchanging the routing information, by changing the routing information by a malicious node, it is possible to change the routing of entire WSN structure or its any network partition. This can be done by altering or changing the routing information, by shortening or extending the route information in the routing table or by generation of false error messages.

6.3.2 Selective Forwarding

Fundamental principle of WSN is ‘Multi-hop”. It means that sensor nodes will forward the entire message to next node in line what they have received. In this attack, nodes drop few messages instead of forwarding everything of what they have received. Attacking nodes deny routing some messages and drop them. If all the packets are denied for forwarding by anode after receiving, is called black hole attack.

6.3.3 Sinkhole Attacks

In this attack attackers seem to be more attractive to its surrounding nodes by forging the routing information. Main aim of attacker is to tempt all the nodes in close proximity, constructive a figurative sinkhole. It results in the malicious node to be most chosen for data forwarding through it by other surrounding nodes.

6.3.4 Sybil Attack

In this attacker attacks a single node in the network with a malevolent code masked with multiple identities. Then this node behaves as polymorphic. Its multiple identities mislead to all other nodes. Some of such identities are decreasing topology maintenance schemes, disparity in storage, disparity in routing.

6.3.5 Wormhole

Wormhole is referred as low latency link between two portions of a WSN network over which an attacker replays network messages [14]. Here an adversary convinces the nodes which are multi hop away that they are closer to the base station (BS).The wormhole attack usually engage two different and far away malevolent codes conspire to minimize their remoteness from each other by replaying packets next to an out-of-reach channel, is only available to attacker.

6.3.6 Hello Flood

Malicious nodes sometime can cause of immense traffic of useless messages. It is known as flooding. Malicious nodes, sometime replay some broadcast traffic which is useless but congest the channel. In hello flood type attack, attackers use very high power RF transmitters to handle the large area of nodes into trusting that they are neighbors of it. Attacker will broadcast a false superior route so that other nodes will attempt very far from it in RF distance.

6.4 Attacks at Transport Layer

6.4.1 Flooding

Any protocol which maintain state at either end, it has to face a problem called flooding. Attacker may repeatedly establish new connection requests until the resources are exhausted, which were required by each connection or reached maximum limit. Under such conditions, further legitimate requests will be ignored. Limiting the number of connections prevents from complete resource exhaustion.

6.4.2 De-synchronization

Connection between two endpoints can be disrupted by de-synchronization. In this attack, the adversary repeatedly forges messages to either or both endpoints. For example, there may be requests for retransmissions of missed frames by the repeated spoof messages. If timed correctly, an attacker may degrade the functionality, capability of end hosts by retransmission of frames unnecessarily. It causes endpoints to waste the energy for attempt to recover from errors which never really exist.

7. WSN CHALLENGES

WSNs. are specific real world problem solving methods not merely as combination of sensor and electronics circuit along with wireless communication linking capability. Many challenges on WSN are to be considered before applying wireless sensors to a particular application, solving a problem

7.1 Resource Constraints

Wireless sensors are low costing, low power tiny devices which may handle and process a limited amount of data , low amount of data transmission capability since transmission require a significant amount of power, very low battery life and memory space. Cause of limited transmission capability bandwidth of channel is also limited resulting limiting radio range of channel. Since it is not possible to replace or recharge the battery of sensor nodes after deployed once, conservation of energy is also to be considered as main factor before designing any software routine or protocol for WSNs.

7.2 Platform Heterogeneity

Wireless sensor network (WSN) may run different applications for different tasks, such as event detection, localization, tracking, or monitoring. Different types of sensor node are therefore required, and to handle heterogeneous WSNs with a large number of these different sensor nodes, comprehensive heterogeneity management architecture is also necessary. When deployed in large networks, sensors, may behave differently due to environment they are deployed in terms of infrastructure or networking technologies. Hence capability and functionality of sensor node may vary.

7.3 Dynamic Network Topology

WSNs may consist of mobile nodes instead of static nodes. Many application demand node mobility such as intelligent transportation, planetary exploration, and animal control. In such solutions new nodes are to added with sleep or replacement on existing nodes. Even after a time period many node me die due to power exhaust. These factors lead to network topology of WSNs to be dynamic, not static. This dynamic topology results in uncertainty of QoS in WSNs.

7.4 Mixed Traffic

Sensor nodes are randomly deployed at large scale to fulfill the requirements of multiple application over heterogeneity. Those application may use or handle the data which are different in nature like as streaming, periods. To meet out such mixed traffic demands WSNs have to be scalable as needed by the applications. However some extra sensor may be required to detect such uncommon properties of applications. Variety of detected inputs or data may vary in size, magnitude, resulting handling of this mixed traffic generated from input of different types of sensors.

7.5 Sensor Deployment and Location:

In WSNs. applications based geographical constraints; require random deployment of sensors in an affected area like as avalanche prone area, volcano prone area. Since sensors are scattered in such critical areas from a distance to be deployed in unknown manner, their position after deployment is uncertain, resulting drastic variance in topology they have formed their selves after deployment. Even some sensor may get damaged or lost during deployment.

7.6 Security

Wireless medium of linking between the node itself is a vulnerability to the architecture due to its easy access to all. Any standard cryptographic strategy or similar one can also not be applied directly to the sensor nodes due to their execution complexity and required many resources like space, memory and energy.

8. WSN SECURITY COMPLICATIONS

Several constraints of the WSN architecture and their low capabilities make security issue complicated in WSN. Physical stealing or capture is one of the issue while securing wireless sensor network. As these network use open air medium for communication, which is easy to penetrate is another security implementation issue with WSN. Any attacker may inject malicious information or data easily into the wireless network. Many anti-jamming techniques are available to eliminate attacks like jamming but those are very complex, energy and processing consuming, hence difficult to be implemented on tiny sensor nodes. Sensors are very tiny, low powered and low processing capable hence more susceptible for DoS attacks. Since sensor nodes form ad-hoc network, attacker may get access to the network easily and can damage the infrastructure.

9. CONCLUSIONS

Limited capability and less capable hardware of WSN nodes make them more susceptible for attacks.

Any traditional security mechanism can also not be applied at any level of WSN architecture to prevent for its respective attacks as nodes will not be able to execute same mechanism or will be exhausting their power and life. Large scale deployment for tightening the security measures are also not possible over low capability nodes. If security is maximized then consumption of resources will increase, result of node's life exhaust. Since sensor nodes usually have severely constrained, asymmetric cryptography is often too expensive for many applications. Thus, a promising approach is to use more efficient symmetric cryptographic alternatives.

REFERENCES

[1]. Al-Sakib Khan Pathan, Hyung-Woo Lee and Choong Seon Hong "Security in Wireless sensor Networks: Issues and Challenges" ISBN 89- 5519-129-4 Feb 22-22, 2006 ICACT2006

[2]. Ritu sharma, Yogesh Chaba and Y.Singh "Ánalysis of Security Protocols in Wireless Sensor Network" International Journal Avanced Networking and Applications Volume 02, issue 03, pages:707-713(2010)

[3]. Neelam Srivastava "Challenges of Next- Generation Wireless Sensor Networks and its impact on Society" JOURNAL OF TELE COMMUNICATIONS, VOLUME 1, ISSUE 1, FEB 2010 128

[4]. Satvika Khanna, Ms. Priyanka Singh, Akhil Kaushik "Wireless Sensor Network: Issues & Challenges" IJMA Vol 2, No 11, 2011

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

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

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

[8]. Kavitha, D. Sridharan "Security Vulnerabilities in wireless Sensor Networks" IJAS 5 (2010)

[9]. 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

[10]. Ian F. Akykildiz et. Al. "A Survey on Sensor Networks", IEEE Communication Magazine, year 2002

[11]. 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, year 2006.

[12]. Chaudhari H.C. and Kadam "Wireless Sensor Networks: Security, Attacks and Challenges" L.U. International Journal of Networking Volume 1, Issue 1, 2011, pp-04-16

[13]. 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.

[14]. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Atttacks and 4 counter measures", In Proceedings of the 1st IEEE Int. Workshop on Sensor Network Protocols and Applications, May 2003