RESEARCH ARTICLE OPEN ACCESS

Denial of Service (DoS) Attacks at Network Layer in WSN

Sunil Ghildiyal, Bhupender Singh Rautela, Anupam Semwal
Uttaranchal University Dehradun Uttarakhand
Graphic Era University Dehradun Uttarakhand
Drona College of Mgmt & Tech. Ed. Dehradun Uttarakhand

ABSTRACT
Recent advancements in technology, tiny size, cost effectiveness have made sensors as a crucial part of real world sensitive applications. These sensor nodes are scattered over an area to monitor the situations like fire, flood and record the data and to forward meaningful data to the center head node for observation, resulting an advance prompt to control the situation. In last decade, WSN have grown significantly in variety of areas and applications, resulted the high, consistent security mechanism. Also, there is variety of attacks on WSN at their different layers of architecture. Though sensor nodes are not capable enough in terms of power, processing etc. but applications based on these sensors demand on-time collection of information or data and then to send same on reliable, secure delivery medium. Small sensors with limited hardware, processing cannot afford traditional security mechanisms to face or sustain the attacks. There is variety of attacks at different layers of WSN architecture to affect sensor's roles like signaling, framing, transmission etc. Many Denial of Service (DoS) attacks are identified at each layer of WSN which are purposeful, planned attacks to hamper the availability of service, restricting the sensor node's utility for problem solution. In this paper we will focus on the WSN architecture, characteristics, constraints and various types of DoS attacks primarily on physical and data link layer and particularly at network layer in details with some suggestions against attacks.

KEYWORDS: Wireless, Sensor, Power, Denial of Service DoS, Attack, Vulnerabilities.

I. 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 sensor nodes[1]. Hence, It becomes very tough to raise the capability level of such tiny sensors due to their various constraints. Constraints, associated 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 a 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 damage purpose[2]. These limited power capacity nodes make WSNs. very weak and paralyzed architecture in front of any intended attack like flooding or replaying etc. One of initial measure against these threats may be authorization access checklist available with them to detect unauthorized or malicious users.

II. 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.

III. WSN CONSTRAINTS

Resource: Sensors are equipped with less capable processors and very low RF linking bandwidth. Of course, It is due to tiny size and low battery. Hence, computational capabilities are also affected by battery and processors.

Memory: A sensor node consists of a flash memory and flash RAM. But loading of operating system and other system applications consume much space, leading less space for other tasks and storage. In sensors, flash memory is used for storing downloaded application code.

Message Size: As compared to any traditional network, message size of WSN is quite small which results in no concept of segmentation in WSN applications usually.

Absence of Global Addressing: As the number of sensors is very large, hundreds or thousands in an application, it is not possible to identify each node with unique addressing at global level.

Location Management: As nodes are small and scattered in an open area, dislocation of nodes by environmental conditions like earthquake or avalanche, mobility of nodes may result in locating the nodes. It affects data to be collected by the nodes after they have been deployed at specific place or have been constant static at same place for a time period.

Data Redundancy: There is very high chance of data redundancy as many nodes may capture the same data of same phenomenon.

Data Availability: It means whether sensor node has the capability to use the resources of network and whether the network is available with the messages to communicate. In WSN, failure of base station or cluster head's availability will also lead to threaten the entire sensor network. Hence it is important to maintain a proper operational network.

Self-Organization: A wireless sensor network is a typically an ad hoc network, where every sensor node is to be independent and flexible enough for self-organization and self-healing under different conditions. WSNs. form random infrastructure as per situation and need network management in a sensor network by nodes themselves.

IV. WSN SECURITY REQUIREMENTS

Ultimate goal of security architecture is to prevent the information from various attacks. Security measures make sure that the services would be available even in presence of DoS attacks or any other vulnerability. It will make sure that only authorized node can be a part of communication of information. As result of it, a malicious node cannot masquerade as trusted node. When authorized users or nodes are exchanging the information, confidentiality must be maintained with data integrity. Data freshness and non-repudiation is also to be considered as main parameters of security measures, whether already applied or to be. WSN nodes are very small and light weight and generally deployed randomly, operated in unattended environment subsequently. Hence the security requirements include self-organization of node which further defines self-configuration, self-management (autonomous) and self-healing (fault tolerant).

V. 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.

VI. WSN ATTACKS

Attacks on WSN can be divided into two categories: invasive and non-invasive. Non-invasive attacks generally target to timings, power and frequency of channel, trying to destroy the signaling system. Whereas invasive type attacks aim to hamper the availability of service, information transition, routing etc. DoS attack aims the system to be inaccessible. However during the transit of information, more common attacks are encountered. Attacks affect the routing schemes, routing tables and routing algorithms mostly in general.

VII. DOS AND DOS ATTACKS

There are varieties of DoS conditions, which may temper the nodes and network operations subsequently. These attacks may hinder the routines of the network, may lead to the resource exhaustion, any software bug, or any difficulty while working with any application or infrastructure. Such obstacles in network functionality are called Denial of Service (DoS) due to its direct affect on availability or fully functionality of service. But when these are because of planned intention of the opponent, these are called DoS attacks.

Dos attacks are intended attack of opponent to destroy the entire network components or operations. DoS attack may limit the network operations more than expected. DoS attack may occur at every layer of OSI layers of WSN [3]. DoS attacks penetrate the efficiency of aimed networks by affecting its associated protocols. DoS 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 DoS attacks first. [4], which was further enhanced by Raymond and Midkiff with some addendums [5]. In this paper, we will discuss about the DoS attacks at different layers of WSN infrastructure in general and then we will conclude with DoS attacks at network layer. .

VIII. DOS ATTACK AT PHYSICAL LAYER

Jamming is one of attack at physical layer, in which radio frequencies used by the network nodes are interfered, adversary can either disrupt entire network which depends on the power of jamming nodes. Jamming is of various types Constant, Deceptive, Random and Reactive [6]. Jamming may be consistent or intermittent.

Another attack at physical layer is tempering, in which attacker may physically temper the nodes and can compromise with them. Temper-proof physical packaging is one alternate of this attack but costs a lot[7].

IX. DOS ATTACK AT LINK LAYER

Exhaustion (Continuous Channel Access is one of major attack where attacker may disrupt the channel by frequently requesting and transmission over it. It results in starvation for channel access for other nodes.

Collision occurs when two nodes intend for same frequency channel transmission simultaneously. Attackers may need to induce a collision instance in one octet of transmission to disturb entire packet transmission.

Unfairness is also one of attack at data link layer which is referred as repeated collision based attack or an abusive use of cooperative MAC layer priority mechanisms.

X. DOS ATTACK AT NETWORK LAYER

X.A. False Routing or Spoofed, Replayed Routing Information

Main focus of such kind of attack is on routing protocols, specifically on routing. Sensor nodes exchange routing information at pre determined time intervals or as per algorithm policy of routing. A malicious node can change routing information, resulting to alter the routing of entire WSN infrastructure or its any partition. This is possible through altering or changing the routing information, by narrowing or extending the routing information in the table or by fake error messages generation. One of best strategy against such attack is to implement MAC code with the message. In addition to it, time stamps can also be added to prevent against replaying the routing.

X.B. Selective Forwarding

Fundamental principle of sensor network is ‘Multi-hop”. It is to ensure that each sensor nodes will forward the entire message to next node in line what they received. In selective forwarding, nodes selectively drop few messages instead of forwarding everything. Attacking nodes deny routing few certain messages and drop them. This attack is effective specially if combined with an attack trying to collect most of the traffic via node. Sensor networks assume that nodes faithfully forward messages what they have received. But some compromised node might refuse to forward packets selectively. As result of it neighbor nodes may opt for alternate route [8].

If all the packets are denied for forwarding by anode after receiving, is called black hole attack. In selective forwarding few messages are dropped and few are forwarded further to the next node. One of the defense mechanism against this attack is multiple paths to send the data.

X.C. Sinkhole Attacks

In this attack attackers seem to be more attractive to its nearby nodes by forging the routing information. Main aim of such attack is to tempt all the neighbor nodes. A sinkhole attack tries to lure mostly all the network traffic toward the compromised node, creating a metaphorical sinkhole with the adversary at the center. Geo-routing protocols are one of the routing protocol classes which are resistant to sinkhole attack, because that topology is based on localized information only and all traffic is naturally routed through the physical location of the sink node [9].

X.D. Sybil Attack

In this attacker attacks a single node in the network with a malevolent code masked with multiple identities or a node duplicates itself and presented in the multiple locations. Then this node acts a polymorphic behavior, misleading to others with multiple identities. Such identities may decrease topology maintenance, disparity in storage and routing or targeting fault tolerant systems. This attack includes a major concern for Geographical Routing Algorithms which needs the location of a node to route the message efficiently. Various authentication and encryption mechanism can prevent an outsider to launch a Sybil attack on the sensor network [10].

X.E. Wormhole

Wormhole is referred as low latency link between two portions of a WSN network over which an attacker replays network messages [11]. An adversary can tunnel messages received in one network partition over a low latency link and replay them in another partition. In such attack, an adversary convinces the nodes which are multi hop away that they are closer to the base station.. The wormhole attack generally involve two far away malevolent codes conspire to minimize their remoteness by replaying packets next to an out-of-reach channel, is only available to attacker.

X.F. Hello Flood

Many protocols require hello packets to announce their neighbors about their state and presence or absence. This attack exploits Hello packets. 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 may also broadcast a fake superior route so that other nodes will attempt very far from it in RF distance. Authentication is the solution to such attacks. Such attacks can easily be avoided by verify bi-directionality of a link.

X.G. Acknowledgment Spoofing

Many routing algorithms used for WSNs require transmission of acknowledgment packets from receiver to sender as a token of successful receipt. Attacking node may spoof the acknowledgements of overheard packet destined for neighboring nodes in order to provide false information to those nodes.

X.H. Node Capture

It is experienced that only single node capture is also more than sufficient for an attacker to take over the entire network and doing malicious action to destroy the network operations.

XI. 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 is 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 can not 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.

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.] Al-sakib Khan Pathan "Denial of Service in Wireless sensor networks: issues and challenges**."**Advances in communications and Media Research ISBN 978-1-60876-576-8.

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

[5.] 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.

[6.] 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.

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

[8.] C. Karl of and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003, pp. 113-127.

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

[10.] Dr. G. Padmavathi, et.a l "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" *(IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009*

[11.] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In Proceedings of the 1st IEEE International Workshop May 2003, pp. 113-127.

[12.] Wang, Q., Zhu, Y. "Reprogramming Wireless Sensor Networks: Challenges and Approaches" IEEE Network, May/June 2006.