International Journal of Academic Research and Development
ISSN: 2455-4197
Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 3; Issue 3; May 2018; Page No. 94-96

Secure routing in a layer wise perspective to attacks & its countermeasure: A survey

Vinkle Sachdeva, Kulbhushan Singla
Department of Electronics & Comm. Gtbkiet, Chhapianwali, Malout, Punjab, India

Abstract
Wireless sensor networks are networks having non wired infrastructure and dynamic topology. In OSI model each layer is prone to various attacks, which halts the performance of a network. In this paper several attacks on four layers of OSI model are discussed and security mechanism is described to prevent attack in network layer i.e. wormhole attack. In Wormhole attack two or more malicious nodes makes a covert channel which attracts the traffic towards itself by depicting a low latency link and then start dropping and replaying packets in the multi-path route. This paper proposes promiscuous mode method to detect and isolate the malicious node during wormhole attack by using Ad-hoc on demand distance vector routing protocol (AODV) with Omni directional antenna. The methodology implemented notifies that the nodes which are not participating in multi-path routing generates an alarm message during delay and then detects and isolate the malicious node from network. We also notice that not only the same kind of attacks but also the same kind of countermeasures can appear in multiple layer. For example, misbehavior detection techniques can be applied to almost all the layers we discussed.
Becoming mature enough to be used for improving the quality of life, wireless sensor network technologies are considered as one of the key research areas in computer science and healthcare application industries. The pervasive healthcare systems provide rich contextual information and alerting mechanisms against odd conditions with continuous monitoring.

Keywords: wireless sensor networks, OSI model, wormhole attack

1. Introduction
Wireless sensor networks sometimes called wireless sensor and actuator networks are spatially distributed autonomous sensor monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. Characteristics of a Wireless sensor networks

2. Open System Interconnection networking suite
In the 1980, the European dominated International Standards Organization begun to build up its Open System Interconnection networking suite. OSI has two major mechanisms a set of concrete protocols and an abstract model of networking. The Open System Interconnection model is isolating a communication system in to smaller parts. These parts are called layers. This model consist seven layers.

2.1 Working of OSI Model Layers
2.1.1 Physical layer
It describes the physical, electrical interpretation of data properties of the communication media. This layer works with hardware element of the communication system. This layer defines the type of BNC connector, size of Ethernet cable and termination method.

2.1.2 Data Link Layer
This is the last second layer of the osi model. It can describe the logical organization of data bits on a particular medium. Data link layer contains two sub layers.
1. Logical link layer
2. Media Access layer.

2.1.3 Network Layer
This layer can exchange the data between two nodes. Network layer is liable for locating destination and calculating optimal path to destination; by tampering with routing services such as modify routing information and replicating data packets.

2.1.4 Transport Layer
This layer discusses about the quality and nature of data delivery and also ensure about the data delivery. These layers define how retransmission is used to make sure data delivery.

2.1.5 Session layer
It provides session building, termination and maintenance. With the help of this the processes between two different machines can be establish and terminate is called a session.

3.3.6 Presentation layer
This layer provides the Character code translation, Data

conversion, Data compression and Data encryption according to the application layer need. This layer formats the data to be presented to the application layer.

3.3.7Application layer
This layer implements the services seen by user like time synchronization and data aggregation. Data aggregation sends data collected by sensor to base station. Time synchronization synchronize sensor clock for cooperative operation.

3. OSI Layer Attacks
3.1 Media Access Control (MAC) flooding
In computer networking, MAC flooding is a technique employed to compromise the security of network switches. Essentially, MAC flooding inundates the network switch with data packets that disrupt the usual sender to recipient flow of data that is common with MAC addresses. Switches maintain a MAC (sometimes called as CAM) Table that maps individual MAC addresses on the network to the physical ports on the switch

3.2 IP spoofing
Attacker uses this method when he wants to send malicious content to target machine and don't wish to get identified. Victim assumes that packet is from trusted host and it accepts packet, response back to source computer. Attacker must guess proper sequence number and if this step gets successful attacker can establish connection with victim's machine.

3.3 UDP Flood
A UDP flood, also known as a fragile, is a cousin to the Smurf attack. This is based on UDP echo and character generator chargen. It uses a forged UDP packet to connect the echo service on one machine to the chargen on another. These two machines then uses up all available bandwidth, sending characters back and forth between themselves.

3.4 Sinkhole
More multifaceted attack than black hole attack. Done by getting certain information of routing protocol in use, the attacker tries to attract from exacting region from side to side it. Attacker announces a false best possible path by advertising attractive power, bandwidth or high quality routes. Other nodes think about that path better than current path and move their traffic on to it.

3.5 Wormhole attack
In the wormhole attacks, a malevolent node excavates the messages it receives at one end of the network over a split low-latency channel. Then it repeats messages at a different point in the sensor network. For example, when a source node is passing on data to a destination node then there can be a mean node in between them which selectively forwards the data packets. The wormhole attacks usually connect two different and far-away malevolent nodes conspire to minimize their remoteness from each other by replaying packets next to an out-of-reach channel which is only available to the invader.

3.6 Clock Skewing
This attack takes place by giving false timing information. This attacks aims to desynchronize the sensors i.e. skewing the clocks. Once modes correct their clock based on memory information they will be out of synchronization with access point

4. Counter Measures
To prevent MAC flooding one of the following features should be configure in switch. Port security: Post security should be configured which limits number of MAC addresses that can be learned on ports connected to end stations. Implementations of IEEE 802.1X suites: It often allow packet filtering rules to be installed explicitly by an AAA server based on dynamically learned information about clients, including the MAC address. B. Session hijacking 1) Theory: It is like taking over secure or unsecure web user session by gaining session ID. Once user session ID is accessed, the attacker can pretend as original user and does anything that user is authorized to do on that network. In case of web communication server send some data to user called as "COOKIE". Cookie is the place where attacker gets session ID of user. This cookie is sent back by user to server when he accesses web for authentication. Attacker gets this cookie and sends to server and pretends as original user

Table 1: OSI Model Layers and its Counter-measure

Layers	Attack types	Countermeasures
Application Layer	Subversion and Malicious Nodes	Malicious Node Detection and Isolation
Data Link Layer	Link Layer Jamming	Link Layer encryption
Physical Layer	DOS and Node capture attacks	Adaptive antennas, Spread Spectrum
Network Layer	Sinkholes, wormholes, Sybil	Routing Loop Key Management, Secure Routing
Transport Layer	Flooding	Manage Connection Request

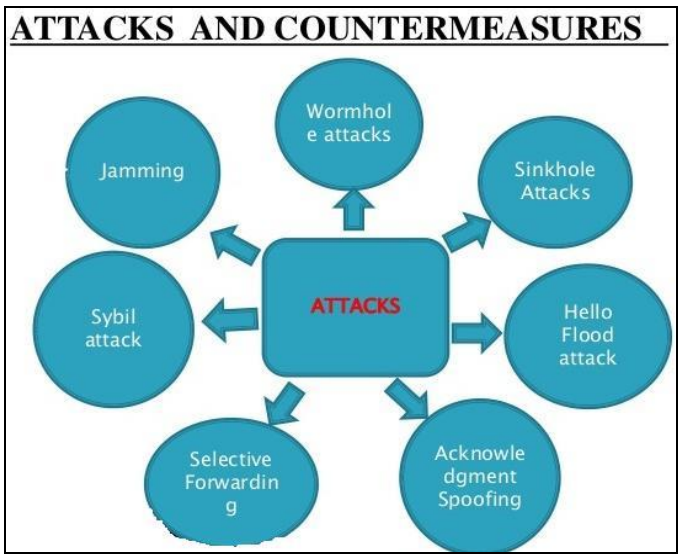

Fig 1: Osi layer Attacks.

5. Conclusions
Promiscuous mode methodology is implemented which works very efficiently in WSNs during wormhole attack. It not only prevents the degradation of the wireless network also helps in improving performance of wireless sensor networks. This methodology has not been proposed yet based on delay

metrics. Analysis has been done through simulation to enhance performance of the proposed model in wireless multihop network. The simulation results have shown that in the presence of malicious nodes in ad hoc network. The performance of wireless network with AODV provided extensions with promiscuous mode mechanism is better than wireless network with simple AODV routing protocol in terms of throughput and end to end delay. Furthermore, it can help in putting some constraints on the network topology to design a robust network for such attacks, and in the design of new and more powerful attack countermeasures. In future more complex attacks can be simulated and comparison of their performances can be done to select the optimum method for prevention of attack from attacker's point of view. Once selected, it will be tested with some of the proposed countermeasures and will help in the development of new attack prevention and detection schemes.

6. References

1. Chris karlof, David Wagner. Security Routing in Wireless Sensor networks; attacks countermeasures,' Elsevier B.V. 2003; 1(2-3):293-315.
2. Al-Karaki JN, Kamal AE. Routing techniques in wireless sensor networks: a survey, IEEE Wireless Communication. 2004; 11(6):6-28.
3. Sulaiman MM, Baig MJ. Secure Routing in Wireless Sensor Network.
4. Renu Bala, Dr. Yashpal Singh. Routing in Wireless Sensor Network, IJIRST-International Journal for Innovative Research in Science & Technology, 2015, 2(01).
5. Joanna Kulik, Wendi Heinzelman, Hari Balakrishnan. Negotiation-based protocols for disseminating information in wireless sensor networks, Wireless Networks-Selected Papers from Mobicom'99. 2002; 8(2/3):169-185
6. Deepak Ganesan, Ramesh Govindan, Scott Shenker, Deborah Estrin. Highly resilient, Energy efficient multipath routing in wireless sensor network, ACM SIGMOBILE Mobile Computing and Communications. 2001; 5(4):11-25.
7. Hande Alemdar, Cem Ersoy. Wireless Sensor Networks for healthcare, Elsevier BV. 2010; 54(15):2688-2710.
8. Tao Shu, Marwan Krunz, Sisi liu. Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes, IEEE Transactions on mobile. 2010; 9(7):941-954.
9. Challal Y, Ouadjaout A, Lasla N, Bagaa M, Hadjidj A. "Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks, Elsevier Ltd. 2011; 34(4):1380-1397.
10. Moshaddique AL, Ameen, Jingwei lui, Kyungsup Kwak. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications, Journal of Medical Systems. 2012; 36(1):93-101.
11. Fenye Bao, Ing Ray Chen, Moon Jeong Chang, Jin Hee Cho. Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection, IEEE. 2012; 9(2):169-183
12. Yanli Yu, Kegiu LI, Wanlei Zhou, Ping LI. Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. 2012; 35(3):867-880
13. Nabil Ali Alrajeh, Shafiullah Khan, Jaime Lloret, Jonathan Loo. Secure Routing Protocol Using Cross-Layer Design and Energy Harvesting in Wireless Sensor Networks, Creative Commons Attribution License, 2012-2013.
14. Madhumita Panda. Security threats of each layer of wireless sensor networks, Ijarcsse. 2013; 3(11):61-67.
15. Santhosh Simon, Paulose Jaiob K. Energy optimized Routing protocol for wirelss sensor network, IJEIT. 2013; 3(4):72-80.
16. Pratyay Kuila,
17. Prasanta Jana K. Energy efficient clustering and routing algorithms for wireless sensor networks: Particle swarm optimization approach. Elsevier Ltd. 2014; 33:127-140.
18. Latha D, Palanivl K. Secure routing through trusted nodes in wireless sensor networks: a survey, IJARCET. 2014; 3(11):3792-3799.
19. Jingsha He, BO Zhou, Ruohong Liu. Analysis of typical secure routing protocols in WSN. 2014; 8:41-50.
20. Mahfuzulhoq Chowdhury, MD Fazlul Kader, Asaduzzaman. Security issue in wireless sensor network: A survey. 2013; 6(5):97-116.
21. Naser Alajmi. Wireless sensor network attacks and solutions, 2014, 12(7).
22. Damandeep Kaur, Parminder Singh. Various OSI layer attacks and countermeasure to enhance th performance of wireless sensor network during wormhole attack, 5(1):62-67.