IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 6, Ver. III (Nov - Dec .2015), PP 10-15
www.iosrjournals.org

A Review of Network Layer Attacks and Countermeasures in WSN

S.Nithya[1], K.VijayaLakshmi[2], V.PadmaPriya[3]
[123]*Department of Electrical and Electronics Engineering SRM University, Ramapuram – Chennai, India*

Abstract: *Wireless Sensor Network is a wireless network of thousands of inexpensive miniature devices capable of computation, communication and sensing. It provides a bridge between real physical and virtual worlds. In spite of its wide range of potential application to industry, science, transportation and security; it poses security threats at different layers. In this paper different types of attacks in network layer are examined and existing solutions were discussed. Some open research issues are also presented.*
Keywords: *Network Layer; Security; Wireless Sensor Network.*

I. Introduction

Wireless Sensor Network are spatially distributed autonomous sensor to monitor physical or environmental conditions[1] such as temperature, sound, pressure etc. and to cooperatively pass their data through the network to a main location.

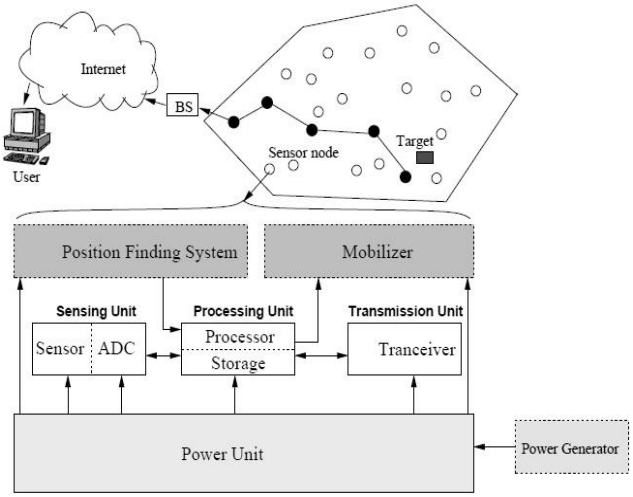

Fig.1.Wireless Sensor Network Architecture

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors.
Each such sensor nodes has several parts: a radio transceiver with internal antenna or connection to external antenna, a microcontroller, an electronic circuit for interfacing with sensors and energy source usually a battery.

The Network Layer has lot of challenges depending on applications, but the major challenges are in power saving, limited memory and buffers. Sensors does not have global ID and have to be self organized. Many security threats in Network Layer have been presented in the literature. In this paper we discuss six important attacks in Network Layer.

The organization of this article is as follows. Section II presents the various security aspect of WSN, section III explains WSN protocol stack, section IV examines different attacks in Network Layer and the existing solutions, section V put forward open challenges in research and final section VI provides conclusion of this paper.

II. Security Aspect Of Wsn

To make a wireless network secure, the network should support all secure parameters like confidentiality, authenticity, availability and integrity.

Confidentiality: - In sensor Network, confidentiality relates to the following [2], [3]

- A sensor network should not leak sensor readings to its neighbors. The data stored in sensor node must be highly sensitive.

- Since the nodes communicate highly sensitive data, secure channel is important in a WSN system.
- The network must encrypt data to protect against traffic analysis attacks.

Integrity: - It ensures that message sent from one node to another is not modified by malicious intermediate nodes. In WSN intrusion detection system can provide integrity mechanism.

Availability: - Attacks damage the availability for WSN for the following reasons

- Additional computation consumes additional energy. If no more energy exists, data will no larger be available.
- A single point failure greatly threatens availability of network if central point scheme is used.

Authenticity: - It ensures that the other end of connection or originator of a packet is the node that is claimed. Access control prevents unauthorized access to a resource.

III. Protocol Stack

A simplified protocol stack for WSN is summarized in figure 2

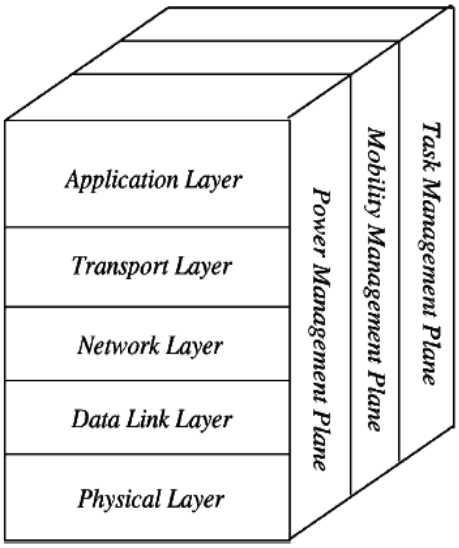

Fig. 2. Protocol Stack

- Application Layer:
  It defines a standard set of services and interface primitives available independently for the programmer on their implementation on every kind of platform.
- Transport Layer :
  It helps to maintain the flow of data, if sensor network application requires it.
- Network Layer :
  It takes care of routing the data, directing the process of selecting paths along which to send the data in the network.
- Data Link Layer:
  It provides multiplexing of data streams, data frame detection and MAC.
- Physical Layer:
  It is responsible for frequency and power selection, modulation and data encryption.

IV. Attacks In Network Layer

The Network Layer vulnerabilities generally fall into one of the two categories: routing attack and packet forwarding attack based on target operation of attacks. The following describes the Network Layer attacks in WSN.

A. Wormhole Attack

In this attack, a pair of colluding attackers record packet at one location and replay them at another location using private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality. Figure (3) shows an example of wormhole attack.

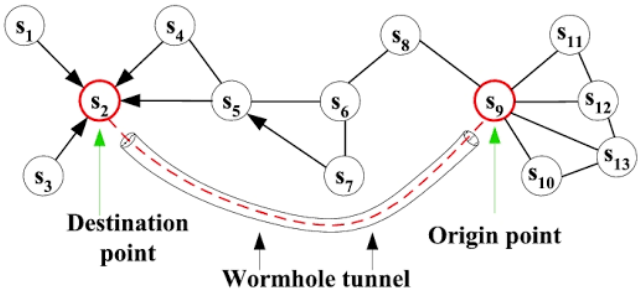

Fig. 3. Wormhole Attack

In [4] packet leashes are proposed to detect and defend against wormhole attack. In [5] the author offers protection against wormhole in OLSR protocol. This approach is based on the location information and requires deployment of public key infrastructure and time stamp synchronization between all the nodes. In [6] the author proposes statistical analysis of multipath which is an approach to detect wormhole attack by using multipath routing..This approach determines the attack by calculating relative frequency of each link in all the routes. The link with highest frequency is identified as wormhole link. The advantage is, it employs limited overhead in multipath routing. But it doesn't work in non –multipath routing protocol like AODV protocol. In [7] the author adopts directional antennas and find infeasible communicating links by utilizing directionality of antenna communication. In [8] author presents a graph based framework to tackle wormholes. This approach assumes existence of guard nodes with extra ordinary communication range. In [9] the author graphically visualizes presence of wormholes. They reconstruct layout of network by centralized multidimensional scaling (MDS) to capture wrap introduced by the wormholes. In [10] the author analyzes impact of combination of wormholes by topology methodology. They locate various wormholes by detecting non separating loops, without any special hardware devices or any assumption on the network properties. In [11] the author explains wormhole attack modes and classes and described attack from attacker's perspective.

B. Flooding Attack

In flooding attack, attacker exhausts network resources such as bandwidth and consume node's resources such as computational and battery power to disrupt routing operation to cause severe degradation in network performance.

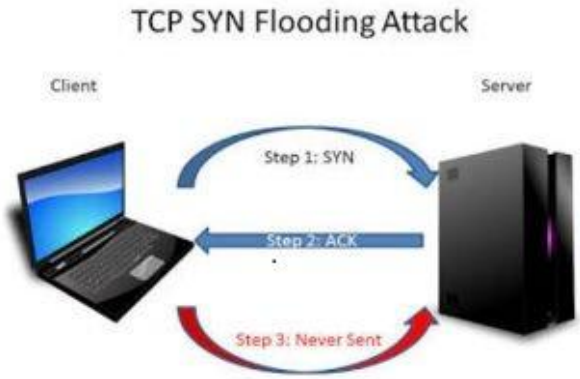

Fig. 4. Flooding Attack

In [12] the author proposes simple mechanism to prevent flooding in AODV protocol. In this approach, each node monitors and calculates rate or neighbor's RREQ. If RREQ rate of any neighbor exceeds predefined threshold, node record ID of this neighbor in the black list and drop any future RREQs from the node. The limitation is, it cannot prevent attack if flooding rate is below threshold. In [13] the author proposed technique based on the statistical analysis to detect malicious RREQ floods. This approach determines threshold based on statistical analysis of RREQs, which can be applied for varying flooding rates.

C. Selective Forwarding / Black Hole

In this attack malicious node behave like normal node and forward packets but selectively drop some packets. When the malicious node acts like a black hole, it drops all the packet passing through it [14]. Selective Forwarding attack is called as special case of Black Hole attack.

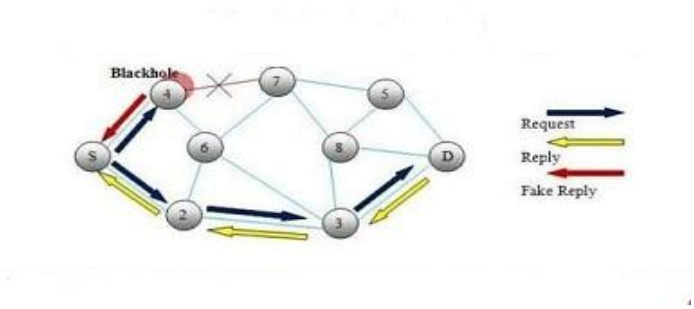

Fig. 5. Black hole Attack

The countermeasures for selective forwarding attack can be classified as follows [15].

- Acknowledgement based detection.
- Detection using neighborhood information.
- Using multidata flow to mitigate attack.

In [16] author describes lightweight detection scheme which uses only two – hop neighborhood information. Each node sends a HELLO packet which contains three important fields source node ID, intermediate node ID and hop counter value. In [17] the author discusses some of the mitigation schemes to defend this attack and also discussed drawback of each scheme. In [18] author analyses four scenarios based on implicit acknowledgement in energy harvesting WSN and proposed hop-by-hop co-operative detection (HCD) to effectively detect the forwarding misbehaviors of malicious node and to mitigate it.

D. Sink Hole

In this, a compromised node is made to look exclusively attractive to its neighbor nodes regarding the routing algorithm and pull almost all the traffic from specific area [19]. The attacker listens route requests of nodes and tries to persuade that it has shortest path for base station [20].

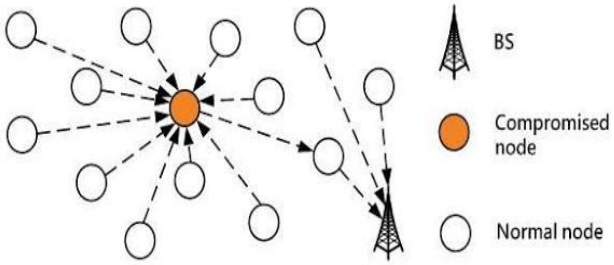

Fig. 6. Sink Hole Attack

In this the author proposed detection scheme based on link quality indicator in sensor network. This method can detect sink hole attack that uses LQI base routing and several detecting nodes. Detecting mechanism is also described in Adhoc networks like AODV [22] and DSR protocol [23]. In [24] author detects malicious node using hop counting. The advantage of this technique is malicious node can be detected without any negotiation with the base station.

E. Sybil Attack

In this attack, single node presents multiple identities to all the other nodes in WSN. This may mislead other nodes and hence route believed to be disjoint with respect to the node can have the same adversary node.

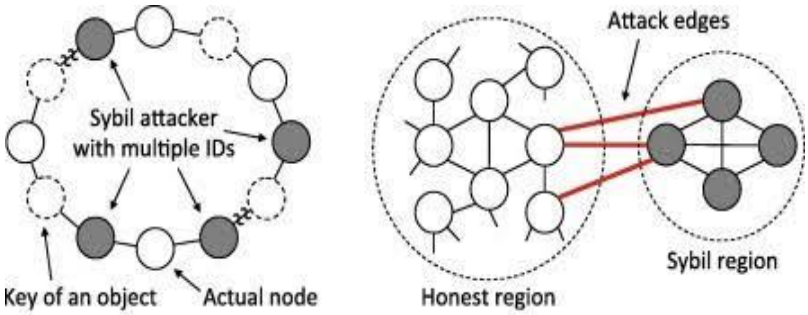

Fig. 6. Sybil Attack

In [25] the author analyses different defenses for Sybil attacks like position verification, registration, key predistribution and code attestation and radio resource testing. In this random key predistribution is most promising methods as it relies on cryptographic principles and robust to compromised nodes. In [26] the author presents a novel decentralized protocol for limiting the corruptive influences of Sybil attacks by bounding both number and size of Sybil groups.

F. Replay Attack

It is a form of network attack, in which a valid data transmission is maliciously or fraudently repeated or delayed. It is carried out either by the originator or by an adversary who intercepts the data and retransmits it.

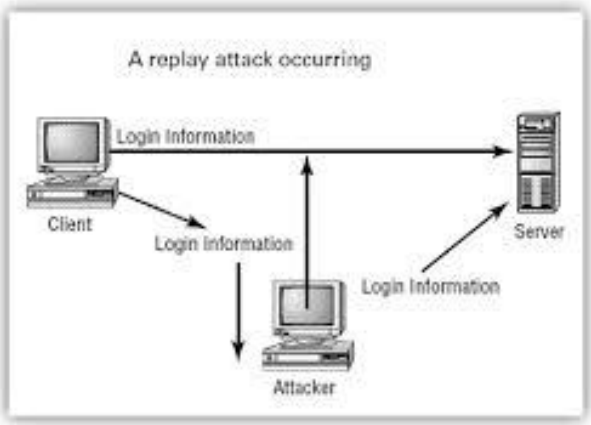

Fig. 7. Replay Attack

There are several countermeasures like session tokens, one Time Password (OTP), Time stamping etc. In [27] the author designs a light weight detection and prevention system cops that intelligently uses combination of digital signatures and Bloom filters to cope with attack.

V. Open Research Issues

Sensor networks are still at an early stage in terms of technique as it is still not widely deployed in world and these provide doors for many research issues. [28], [29], [30]

- Energy efficiency is an important criterion. It is necessary to find the energy efficient routes to improve the life time of network.
- Data collected by various sensors in WSN are typically based on common phenomena. Hence there is a high probability, that this data has some redundancy.
- Multipath design technique must be incorporated. So that a path among them can be used, when the primary path fails.
- Sensor network collect information from physical environment and are highly data centric. To maximize energy saving a flexible platform for performing routing and data management must be provided.
- Messages exchanged in WSN are vulnerable to security attacks. During transmission, messages can be tampered or eavesdrop. Research is needed to ensure the confidentiality of messages.

VI. Conclusion

WSN are having extraordinary growth nowadays because of its application in various fields. The application using WSN, expects guarantee in security in all aspects. In this paper various attacks in Network layer were discussed and different existing countermeasures to overcome these attacks were reviewed. But the recently offered security mechanism are relayed on particular network structure, hence it is less efficient to provide complete solution for security in WSN. This paper has suggested some open research challenges in this regard.

References

[1]. "Environmental and Temperature Monitoring", Centrak.
[2]. F.Akyildilz, W. Su. Y. Sankrasubramaniyam and E. Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, 40(8): 102 – 114, August 2002.
[3]. Erdal Cayirci and Chenming Rong, "Security in Wireless Adhoc and Sensor Networks", A John Wiley and Sons Ltd, Publication, 2009.
[4]. Y.Hu, A.Perig and D. Johnson, "Wormhole Attack in Wireless Networks", IEEE JSAC, Vol 24,no. 2, Feb. 2006.
[5]. D.Raffo et al, "Securing OLSR Using Node Locations", proc. 2005. Euro, Wireless, Nicosia, Cyprus, Apr. 10-13, 2005.
[6]. L. Qian, N. Song and X. Li, "Detecting and Locating Wormhole Attack in Wireless Adhoc Network Through Statistical Analysis of Muitipath",IEEE, Wireless Communication and Networking Conference.'05.
[7]. L.Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", presented at NOSS, 2004
[8]. R. Poovendhan and L. Lazos, "A Graph Theoritic Framework for Preventing Wormhole Attack in Wireless Adhoc Networks", Wireless Networks.Vol 13, pp. 27-59, 2007.
[9]. W.Wang and B. Bhargava,"Visualization of Wormholes in sensor Networks",in proc. ACM wise, 2004, pp. 51-60.
[10]. Dezun Dong, Mo Li, Yanhao Li and Xiang – Yang, "Topological Detection on Wormholes in Wireless AdHoc and Sensor Networks", IEEE transactions on Networking, Vol 19, No 6, pp. 1787-1795. Dec. 2011
[11]. Azer,Sherif,Magdy, "A Full Image of Wormhole Attacks Towards Introducing Complex Wormhole Attacks in Wireless Adhoc Networks", IJCSIS, Vol 1, No 1, pp. 41-51, May 2009.
[12]. P. Yi et al, "A New Routing Attack in Mobile Ad Hoc Networks", int. J. Infotech, Vol. 11, no 2, 2005.
[13]. S.Desilva and R.V.Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks", proc. IEEE Wireless Communication and Networking Conference, New Orleans, LA, 2005.
[14]. Chris Karlof and David Wagnet, "Secure Routing in WSN: Attacks and Countermeasures Ad Hoc Networks 293-315, 2003.
[15]. L. K. Bysani and A. K. Tureek,"A Survey on Selective Forwarding Attack in WSN", in Devices and Communications, 2011, International Conference on IEEE, 2011,pp. 1-5.
[16]. Trian Hoang Hai and Eui Nam Huh, "Detecting Selective Forwarding Attacks in WSN Using TwoHop Neighbor Knowledge", In NCA pages 325 –331, 2008.
[17]. Jaspreet Singh,Anuj Gupta, "Different Approaches to Mitigate Selective Forwarding Attacks in WSN", IJIET, Vol 3, pp. 40-46, 2014.
[18]. Sunho Lim and Lauren Huie,"Hop-by-Hop Co-operative Detection of Selective ForwardingAttacks in Energy Harvesting WSN"' ICNC,Workshop on CNC, on IEEE, 2015, pp. 315-319.
[19]. Hemanta Kumarand Avijit Kar,"Wireless Sensor Network Security Analysis", international Journal of Next Generation Networks (IJNGN),Vol. 1, No. 1, Dec. 2009.
[20]. E. C. Nagai, J. Liu and M. R. Lyer, "An EfficientIntruder Detection Algorithm against Sink Hole Attacks in WSN", Computer Communications, Vol. 30, no. 11, pp. 2353-2364, 2007.
[21]. B. G. Choi, E. J. Cho, J. Hokim, C. S. Hong and J. H. Kim, "A Sink Hole Attack Detection Mechanism for LQI Based Mesh Routing in WSN", ICOIN 2009,pp. 1-5.
[22]. D.Dallas,C. Leckie and K.Ramamohanrao, "Hop Count Monitoring: Detecting Sink Hole Attack in WSN", ICON 07: Proceedings of 15th IEEE International Conference. 2007, pp. 176-181.
[23]. A. A. Pilzada and C. M. C. Donald, "Circumventing Sinkhole Attacks in WSN Using Hop Count", I.J.Computer Network and Information Security, 2015,pp. 50-56.
[24]. Md.Ibrahim, Md.Muntasir, "Detecting Sink HoleAttacks in WSN using Hop Count", I.J. ComputerNetworks and Information Security, 2015,pp. 50-56.
[25]. James Newsome,Elaine Shi,Dawn Song,and Adrian Purig,"The Sybil Attack in Sensor Networks:
[26]. Analysis and Defenses", April 26-27, 2004,Berkely,California, USA.
[27]. Haifeng Yu, Michael, Philip and Abraham, "Sybil Guard: Defending Against Sybil Attacks in SocialNetworks", SIGCOMM '06, Sep. 11-15.
[28]. Navnet, Rakesh, "Sybil Attack Detection and Prevention Using AODV in VANET", IJCSM, Vol 13, Sep. 2013.
[29]. Limin Wang, "Survey on Sensor Networks", Department of Computer Science Engineering,Michigan State University, 2004.
[30]. Deepak Ganesan et al, "Networking issues in Wireless Sensor Networks", Elseiver Science, 9thDecember 2006.
[31]. P.Jiang, yu Wen et.al, "A Study of Routing Protocol in Wireless Sensor Networks", in Proceedings of 6th World Congress on intelligent Control and Automation, June 21-23, 2006, Dalian, China.