National Conference on Innovative Trends in Science and Engineering (NC-ITSE'16)
Volume: 4 Issue: 7
ISSN: 2321-8169
398 - 401

Network Layer Attacks in Wireless Sensor Network: A Review

Ravikiran G. Deshmukh
Department of CSE
MGI-COET,
Shegaon, Maharashtra, India
Ravideshmukh611@gmail.com

Deepika A. Kadale
Department of CSE
MGI-COET,
Shegaon, Maharashtra, India
deepikakadale@gmail.com

Kshitij R. Mawle
Department of CSE
MGI-COET,
Shegaon, Maharashtra, India
krm.mawale@gmail.com

Pravin V. Thakare
Department of CSE
MGI-COET,
Shegaon, Maharashtra, India
pravint275@gmail.com

Gaurav D. Gulhane
Department of CSE
DRGIT& R,
Amravati, Maharashtra, India
gdgulhane@gmail.com

***Abstract*—**Wireless Sensor Network (WSN) is a growing technology that shows great promise for several futuristic applications such as mass public and military purposes. The sensing technology combined with processing power and wireless communication makes it beneficial for being exploited in wealth in future. The presence of wireless communication technology also incurs various types of security threats. The objective of this paper is to investigate security related issues and challenges in wireless sensor network and different types network layer attacks in wireless sensor networks.

Keywords- Wireless Sensor Network, sensing technology, security threats, network layer attacks.

*****

I. INTRODUCTION

Wireless Sensor Networks (WSNs) consist of spatially disseminated autonomous small devices that supportively monitor environmental or physical conditions in remote and often inimical environments. WSNs as a special case of Mobile Ad-Hoc Networks (MANETs) are originally inspired by military applications such as border surveillance and battlefield monitoring. Nowadays WSNs can be used in many civilian applications, like home automation, traffic control, health care and habitat environment monitoring.

Wireless Sensor Networks have several unique features that make them distinguishable from traditional wireless networks. Initially, WSNs generally operate in unattended areas and contain a large number of sensor nodes, which can be in the order of thousands nodes. These nodes have strictly limited resources in terms of energy, memory, communication and computational power. Due to such resource constraints, reliability and precision of a single wireless sensor node is considerably low thereby requiring collaborative data collecting and processing. Also, because of the simple and unreliable hardware, sensor nodes may expire earlier than their expected lifetime. Hence, the number of sensor nodes may also get changed in the network lifetime in a dynamic changing topology. In order to use WSNs in real world applications, these unique characteristics of WSN must be carefully addressed during the protocol design [1, 2].

Security is another unique characteristic of WSNs and it is a fundamental concern in order to provide protected and authenticated communication between sensor nodes in mission critical applications, such as military or healthcare organisation. As in any other wireless network (e.g. cognitive radio networks or radio frequency identification networks), basic security services of WSNs includes authentication, Secrecy, confidentiality, integrity, anonymity and availability. On the other hand, in contrast to traditional wireless networks, in WSNs, physical security of wireless sensor nodes are not fixed as they are usually installed in remote and hostile locations. Hence, attackers can easily compromise sensor nodes and use them to reduce the network's performance. Due to absence of physical security, the existing security solutions that are settled for traditional wireless networks cannot be directly used in WSNs. Also, because of the unique properties of WSNs, their security mechanisms must be developed during system design process [3, 4].

The rest of the paper is as follows: Section 2 describes the design issue of WSN followed by in section 3 basic security schemes in WSN are highlighted. In section 4 classification of attacks in network layer is given followed by conclusion in section 5.

II. LITERATURE SURVEY

Sr. No.	Author's Name	Evolution Approach
1.	M. Marina and S. Das	i. proposed Ad hoc On-demand Multipath Distance Vector (AOMDV) routing protocol. ii. AOMDV extends the Ad hoc On-demand Distance Vector (AODV) protocol to discover multiple paths between the source and the destination in every route

		discovery. iii. The message overhead in the route discovery, and route maintenance is high in AOMDV because of its on demand nature of routing in static topology natured WSNs.
2.	K. Guan and L. M. He	i. proposed energy-efficient multi-path routing protocol for WSNs. ii. The route discovery mechanism provides the multiple paths between the source and destination using shared nodes in the query tree and search tree. iii. The number of control message packets used in the multiple route construction is high to construct a query tree and a search tree.
3.	C. S. Nam, H. Y. Cho, and D. R. Shin	i. Proposed an efficient path set up and recovery in WSNs. ii. This mechanism finds the optimal path between the source and destination based on the minimum number of hops but setting up of the multiple paths is not shown.
4.	M. Radi	i. Proposed Low-Interference Energy-Efficient Multipath Routing (LIEMRO) for WSNs. ii. Uses load balancing based on the average interference level, average residual battery and Estimated Transmit Energy (ETX) value of each path. iii. Usage of neighbouring control signals and separate route request packets for each path in the network demands high control overhead in the network.
5.	M. Bheemalingaiah, M. M. Naidu, D. S. Rao, and G. Varaprasad	i. Proposed Power-Aware Node-Disjoint Multi-Path Source Routing (PNDMSR) protocol. ii. Having disadvantage, if the network is dense, identifying the multiple node disjoint paths is cost effective. The number of control messages used may be higher.
6.	S. Kumar and S. Jena	i. Proposed Secure Cluster Based Multipath Routing Protocol (SCMRP) a proactive, hierarchical multipath secure routing protocol. ii. The SCMRP model sends NeighBouR DETection (NBR DET) packet to construct the neighbour list in each node. iii. These packets, neighbour list and pair-wise key received by the base station consume high energy in the resource constrained WSNs.

III. DESSIGNING ISSUES FOR WIRESS SENSOR NETWORK

The nature of large, ad-hoc, wireless sensor networks presents significant challenges in designing routing schemes. A wireless sensor network is a special network which has many constraint compared to a traditional computer network. Due to the reduced computing, radio and battery resources of sensors, routing protocols in wireless sensor networks are expected to full fill the following requirements [4].

A. Autonomy: The assumption of a dedicated unit that controls the radio and routing resources does not stand in wireless sensor networks as it could be an easy point of attack. As there will not be any centralized entity to make the routing decision, the routing procedures are delivered to the network nodes.

B. Energy Efficiency: Routing protocols should persist network lifetime while upholding a good mark of connectivity to allow the communication between the nodes. It is important to note that the battery replacement in the sensors is infeasible since most of the sensors are distributed. Under some circumstances, the sensors are unreachable. For example, in wireless underground sensor network, some devices are deployed to make them able to sense the soil.

C. Scalability: Wireless sensor networks are composed of thousands of nodes so routing protocols should work with this amount of nodes.

D. Fault-tolerant: Sensors may unpredictably stop operating due to environmental reasons or to the energy consumption. The Routing protocols should deals with this eventuality so when a current node fails, an alternative route should be discovered.

E. Device Heterogeneity: Although most of the applications of wireless sensor network depends on on homogenous nodes, the introduction of different kind of sensors could report significant benefits. The use of nodes with different transceivers, processors, power units or sensing components may improve the characteristics of the network. Comparing with other networks, the scalability of the network, the energy drainage or bandwidth is very latent to benefit from the heterogeneity of nodes.

F. Mobility Adaptability: The different applications of wireless sensor networks could demand nodes to deals with their mobility, the mobility of the sink or the mobility of the event to sense. Routing protocols should provide appropriate support for these movements. [5][6]

IV. SECURITY THREATS AND ISSUES IN WIRELESS SENSORS NETWORKS

Most of the threats and attacks against security in wireless networks are almost comparable to their wired counterparts while some are exacerbated with the inclusion of wireless connectivity. In fact, wireless networks are usually more susceptible to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the directed transmission medium. The broadcast nature of the wireless communication is a simple candidate for eavesdropping. In most of the circumstances various security issues and threats related to those consider for wireless ad hoc networks are

also applicable for wireless sensor networks. These issues are very well enumerated in some past researches and also a number of security schemes are already been proposed to fight against them. However, the security mechanisms devised for wireless ad hoc networks could not be applied directly for wireless sensor networks because of the architectural disparity of the two networks. Where-as ad hoc networks are in self-organizing nature, dynamic topology, peer to peer networks formed by a collection of mobile nodes and the centralized entity is absent, the wireless sensor networks could have a command node or a base station (centralized entity termed as a sink). The architectural aspect of wireless sensor network could make the employment of a security schemes little bit easier as the base stations or the centralized entities could be used extensively in this case. Though, the major challenge is induced by the constraint of resources of the tiny sensors. In many cases, sensors are assumed to be deployed arbitrarily in the enemy territory (especially in military investigation scenario) or over dangerous or risky areas. Therefore, even if the base station (sink) resides in the friendly or safe area, the sensor nodes want to be protected from being compromised.

Attacks in Wireless Sensor Networks

Occurrences against wireless sensor networks could be broadly considered from two different levels of views. One of the attack is against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). Here some of the major attacks in wireless sensor networks, points out in table 1 are describe bellow.

Table1: TYPES OF ATTACK ON NETWORK LAYER [5,6]

ATTACK	DEFINITION	EFFECT
Black hole	In a black hole, the attacker swallows all he receives, just as a black hole absorbing everything passing by.	-It can disrupt the communication between the base station and the rest of the wsn, and hence prevent the wsn from serving its purpose. -Throughput of a subset of nodes, around the attacker and with traffic through it, is decreased.
Wormhole	A Wormhole attack requires two or more adversaries have better communication resource than normal nodes, and can establish better communication channels between them.	-False routing information. -Change the network topology. -Packet destruction/alteration by wormhole nodes. -Changing normal messages stream.
Sybil	In Sybil attack, a malicious node attract by representing multiple identities to network.	-Confusion and WSN disruption. -Enable other attacks. -Exploiting the routing race condition.
Sinkhole	Sinkhole is a more complex attack compared with black hole attack.	-Attracts almost all the traffic. -Triggering other attacks, such as eavesdropping, trivial selection forwarding, black hole and wormhole. -Changes the base station's position.
Selective forwarding	In Selective forwarding attack, attacker refuses to forward packets or selectively drops them and acts as a black hole.	-Message modification. -Information fabrication and packet forwarding. -Suppressed message in a certain area. -Routing information of modification. -Exhaustion of resources.
Hello flood	In Hello flood attack, attacker broadcast hello message with strong transmission power to the network and acts as a fake sink.	-Create an illusion to base station of being a neighbor to many nodes in the network. -Confuse the network routing badly.
Acknowledgement spoofing	Attacker routes the packets to false destination, create the loops in the networks.	-False and misleading messages generated. -Resource exhaustion. -Degrade the WSN performance.

V. CONCLUSION

Wireless sensor networks are vulnerable to wide range of security attacks because of their deployment in an open and unprotected environment. This paper introduces the major security threats in WSN and also investigates different network layer attacks detection techniques. It has been studied that among the number of techniques discussed, each technique has its own strength and weaknesses and there is no proper attack detection technique that can detect all network layer attacks completely. For detecting such type of attack one needs special security scheme except existing ones because disadvantage of the lack of processing,

memory and battery power. Therefore, designing such type of security scheme is still an open research challenge.

REFERENCES

[1] M. Tubaishat, S. Madria, (2003) "Sensor Networks : An Overview ", IEEE Potentials, April/May 2003

[2] Jamal N. Al-Karaki & Ahmed E. Kamal, (2004) "Routing Techniques in Sensor Networks: A survey", IEEE communications, Volume 11, No. 6, Dec. 2004, pp. 6-28.

[3] Al-Sakib khan Pathan et.al,(2006) "Security in wireless sensor networks: Issues and challenges" in feb.20-22,2006,ICACT2006,ISBN 89-5519-129-4 pp(1043-1048)

[4] H. Mohammadi, E.N. Oskoee, M. Afsharchi, N. Yazdani, and M. Sahimi. "A percolation model of mobile ad-hoc networks," International Journal of Modern Physics C (IJMPC), vol. 20, no.12, pp. 1871−902, 2009.

[5] Ms. Priya Maidamwar, N. A. Chavhan "A Survey on Routing Techniques for Wireless Sensor Networks", 2012 National Conference on Innovative Research Trends in Computer Science Egg. & Technology

[6] Ms. Priya Maidamwar, N. A. Chavhan "A SURVEY ON SECURITY ISSUES TO DETECT WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK", International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 4, October 2012

[7] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., "Analyzing interaction between distributed denial of service attacks and mitigation technologies", Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003, pp. 26 – 36.

[8] Douceur, J. "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (2002). [9] Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.

[9] Culpepper, B.J. and Tseng, H.C., "Sinkhole intrusion indicators in DSR MANETs", Proc. First International Conference on Broad band Networks,

2004, pp. 681 – 688.

[10] Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.

[11] Hu, Y.-C., Perrig, A., and Johnson, D.B., "Packet leashes: a defense against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.