International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com‖ Volume 2 Issue 4‖ April 2016 ‖ PP 50-54

Detection & Prevention Techniques of Sinkhole Attack in Mobile Adhoc Network: A Survey

Neelam J. Patel
[1](*Ph.D. Research Scholar, CSE Dept., ASET, Amity University Haryana, INDIA.*)

ABSTRACT: Sinkhole attack is one of severe kind of attack in wireless sensor network. Sinkhole attack tries to attract network traffic toward them by advertising un-authorized routing updates and reduce the performance of network. Sinkhole attacks are capable of performing to launch other attacks on the network such as selective forwarding and wormhole attacks. This paper focuses on exploring and analysing the surviving solution which uses to detect and prevent sinkhole attack in wireless sensor network. The analysis is based on used techniques, Function of Algorithm and parameter compared.

KEYWORDS - Ad hoc On Demand Distance Vector (AODV), base station (BS); Destination-Sequenced Distance-Vector (DSDV), wireless sensor network (WSN).

I. INTRODUCTION

A wireless sensor network (WSN) consists of hundreds of thousands of tiny autonomous sensor nodes that can sense condition of surrounding environment for example illumination, humidity and temperature. Each sensor node is deployed and transmits data to base station (BS).The application of wireless sensor networks are broad like environmental monitoring, acoustic detection, and seismic detection, military surveillance, inventory tracking, medical monitoring, smart space, etc. Wireless sensor network is more vulnerable to attacks. There is difference type of attacks in WSNS, categorize these attacks based on their impacts, including data integrity and confidentiality, power consumption, routing, identity, privacy, and service availability.

Our main focus is on attacks against the routing protocol in Wireless sensor networks. Routing attacks have the aim of modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. Wireless communication is broadcast by nature. A common radio signal is easy to jam or intercept. An attacker could overhear or disrupt the service of a wireless network physically. There are lot of attacks on these networks which can be classified as routing attacks and data traffic attacks. Some of the data attacks in sensor nodes are wormhole, jamming, selective forwarding, sinkhole and Sybil attack. Sinkhole attack can construct the bogus route in network and provide wrong information to nodes so network disturb their topology and make over heading.

II. SINKHOLE ATTACKS

Sinkhole attacks are network layer attack. It is based on misleading the data traffic path exploits it for its benefit in modifying or destroying the secret information [1]. Sinkhole can executes many other attacks like selective forwarding, black hole attacks. A sinkhole attack in WSN can cause serious problem in the processes and services of the networks. It may lead to the problem of system miscarriage in term of network accessibility and it makes the sensor node unable to transmit and receive information [2].

Sinkhole attacks normally work by creating a compromised node look attractive to neighbouring nodes with detail to the routing algorithm. It is accomplished by advertising itself as the highest quality or shortest route to base station. Most of the routing protocols like Destination-Sequenced Distance-Vector (DSDV) Routing Protocol, Ad hoc On Demand Distance Vector (AODV) Routing Protocol, Mint Route and Multi hop LQI [17] are specially designed for WSNs. For a challenger to publicise a high quality route which is imaginary, it could perform spoofing or replay an attacks. Some established advertisements of some other nodes in the network can be repeated by the attacker to announce itself with a high quality route to base station. Each nearest node of the challenger will forward packets bound for a particular purpose destination for a BS through the sinkhole node, and also broadcast the lure of the route to its neighbours. Now the whole traffic propagated through BS will be forwarded to the sinkhole node which can modify, drop or selectively forward the BS, and the BS is disallowed from achieving complete and accurate data. Fig.1 shows a network with a sinkhole next to the base station.

Sinkholes normally a rasp rung nearer to the BS so that the sinkhole node can disturb the entire sub area in which compromised node exists.

III. SINKHOLE DETECTION TECHNIQUES:

1. Leader based intrusion detection system [3]
2. Based on control packet and energy consumption [4]
3. Mobile agent based approach [5]
4. Ad-hoc demand distance vector (AODV) routing protocol [6]
5. Data consistency and network flow information approach [7]
6. Using message digest algorithm [10]
7. Fuzzy rules based detection [8]
8. Hop count monitoring scheme [9, 19]
9. AODV Based Secure Routing Algorithm against Sinkhole Attack [2]
10. Truthful Detection of Packet Dropping Attack [18]
11. Based on redundancy mechanism detect sinkhole attack [21]

IV. PREVENTION BASED APPROACHES:

1. A message digests algorithm using cryptography to detect sinkhole attacks [10]
2. Two protocols, RESIST-0 and RESIST-1, which use a cryptographic approach in routing protocols to address the problem of sinkhole attacks [11, 12]
3. A Trust Based Routing Protocol for Mitigation of Sinkhole Attacks in Wireless Sensor Networks [13]

V. HYBRID APPROACHES:

1. To detect sinkhole and sleep deprivation attacks to combines anomaly and signature-based detection hybrid Intrusion system [14]
2. To detect sinkhole attacks using Radio Signal Strength based Intrusion method (RSSI) [15]
3. Secured and Intelligent Multipath Routing Approach using AOMDV [22]

VI. FIGURE :

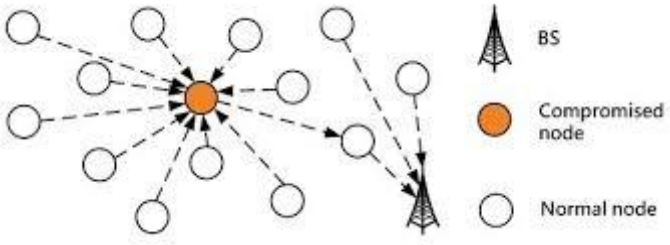

FIG 1: SINKHOLE ATTACK [16]

VII. TABLE:

Paper No., Author and year	Techniques used	Use or Function of Algorithm	Direction of Future Work	Parameter compared
S. Sharmila et al. [2011]	Message Digest Algorithms [11]	To detect Sinkhole attack & provide trustable route Tested in MATLAB	Simulate it in NS2 OR NS3 in term of network throughput ,routing overhead and communication cost	Success rate, false positive rate and false negative rate
Maliheh Bahekmat, et al. [2012]	A Novel Algorithm in term of energy consumption [4]	To detect Sinkhole attack	The proposed algorithm can be used for detection of wormhole	No. of rounds and detection of sinkhole nodes

			attack	
Udaya Suriya Rajkumar et al. [2013]	A Leader Based Intrusion Detection System(LBIDS) [3]	To detect and avoid sinkhole attack	To improving the energy efficiency of the network lifetime of the network	No of nodes and no of detected attacker
Ahmad Salehi S. et al. [2013]	Data consistency and network flow information approach [7]	To detect sinkhole attack	Further improved specially in greater effective statically algorithms	Success rate or false negative rate and ratio of colluding nodes
Fang-Jiao Zhanga et al. [2014]	Redundancy based mechanism [21]	To proposed a new sinkhole detection algorithm based the multi-path selection	To perfect the algorithm raised continuously and extensively	Comparison of detection rates based on multi-path detection
Md. Ibrahim Abdullah et al. [2015]	Hop count [19] monitoring scheme	To detect Sinkhole attack for large sensor field	Applicable to detect wormhole attack and also applicable when sinkhole nodes advertise high quality link, strong transmitted power	Compared the average hop distance with lowest hop distance. To find an optimum value of threshold
Van dana B et al. [2015]	AODV based secure routing algorithm [2]	To detect sinkhole attack by finding the difference of nodes sequence numbers using threshold value	Developed secure AODV (SAODV) routing algorithm to detect different attacks	Performance metrics as Throughput, PDR and Packet loss using NS2
Noble George et al. [2015]	SAODV based truthful detection of packet dropping attack [18]	Truthfully detect packet dropping attack	To perform corrective action against packet dropping	Compared to AODV, SAODV have very high detection rate.
Omid Naderi et al. [2015]	An entropy based trust model [13]	To presented an efficient algorithm to mitigate the effects of sinkhole attacks	To utilizes an adaptive routing protocol	Effectiveness against sinkhole attack and selective forwarding , and the gain resilience to packet dropping by the malicious nodes
Rashmi Gupta et al. [2016]	Secured and Intelligent Multipath Routing using AOMDV Algorithms [22]	Minimizing energy consumption of the nodes and secure of sensor nodes	To improve securities in sensor nodes using other cryptography techniques.	To Compared the results of RSA and Diffie Hellman Algorithms in term of time

		using cryptographic algorithms RSA and Diffie Hellman		taken

TABLE: COMPARISON OF DIFFERENT SINKHOLE DETECTION & PREVENTION TECHNIQUES

VIII. CONCLUSION

One of the main challenges in the design of routing protocols for WSNs is energy efficiency due to the scarce energy resources of sensors. The ultimate objective behind the routing protocol design is to keep the sensors operating for as long as possible, thus extending the network lifetime. The energy consumption of the sensors is dominated by data transmission and reception. Therefore, routing protocols designed for WSNs should be as energy efficient as possible to prolong the lifetime of individual sensors, and hence the network lifetime.

REFERENCES

[1]. Dr.Nabeel Zanoon, Dr. Nashat Albdour et al., "SECURITY CHALLENGES AS A FACTOR AFFECTING THE SECURITY OF MANET: ATTACKS AND SECURITY SOLUTIONS", International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.3, May 2015

[2]. Vandana B. Salve, Leena Ragha et al., "AODV Based Secure Routing Algorithm against Sinkhole Attack in Wirelesses Sensor Networks", IEEE-2015, 978-1-4799-6085-9/15

[3]. Udaya Suriya Rajkumar, D and Rajamani Vayanaperumal, "A Leader Based Monitoring Approach for Sinkhole Attack inWireless Sensor Network", Journal of Computer Science 9 (9):1106-1116, 2013, pp 1106-1116. ISSN: 1549-3636

[4]. Maliheh Bahekmat, et al, "A novel algorithm for detecting Sinhole attacks in WSNs", International Journal of Computer Theory andEngineering, Vol. 4, No. 3, June 2012, pp 418-421

[5]. D. Sheela, et al, "A non Cryptographic method of Sink hole attackDetection in Wireless Sensor Networks", IEEE-InternationalConference on Recent Trends in Information Technology, June 3-52011, pp 527-532

[6]. Tejinderdeep Singh and Harpreet Kaur Arora,"Detection and Correction of Sinkhole Attack with Novel Method in WSN Using NS2 Tool", International Journal of Advanced Computer Scienceand Applications, Vol. 4, No. 2, 2013, pp 32-35

[7]. Ahmad Salehi S., et al., Detection of Sinkhole Attack in Wireless Sensor Networks "Proceeding of the 2013 IEEE InternationalConference on Space Science and Communication (Icon Space)", 1-3 July 2013, pp 361-365

[8]. Murad A. Rassam., et al., A Sinkhole Attack Detection Scheme in Mint route Wireless Sensor Networks, 1st IEEE International Symposium on Telecommunication Technologies, 26-28 Nov2012, pp 71-75

[9]. Daniel Dallas, Christopher Leckie, Kotagiri Ramamohanarao; "Hop-Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks", 15th IEEE International Conference on Networks, 2007, ICON 2007, pp. 176-181

[10]. S. Sharmila and G. Uma maheswari, "Detection of Sinkhole Attack in Wireless Sensor Networks Using Message Digest Algorithms", 2011 International Conference on Process Automation, Control and Computing, (2011), pp. 1-6

[11]. A. Papadimitriou, F. Le Fessant, A. C. Viana and C. Sengul, "Cryptographic protocols to fight sinkhole attacks on tree-based routing in Wireless Sensor Networks", 2009 5th IEEE Workshop on Secure Network Protocols, (2009), pp. 43-48

[12]. F. Le Fessant, A. Papadimitriou, A. C. Viana, C. Sengul and E. Palomar, "A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis," Comput. Commun., vol. 35, no. 2, (2012) January, pp. 234–248

[13]. Omid Naderi, Mahdi Shahedi et al., "A Trust Based Routing Protocol for Mitigation of Sinkhole Attacks in Wireless Sensor Networks", International Journal of Information and Education Technology, Vol. 5, No. 7, July 2015

[14]. L. Coppolino, S. D'Antonio, L. Romano and G. Spagnuolo, "An Intrusion Detection System for Critical Information Infrastructures using Wireless Sensor Network technologies", 2010 5th International Conference on Critical Infrastructure (CRIS), (2010), pp. 1-8

[15]. W. R. Pires Junior, T. H. de P. Figueiredo, H. C. Wong and A. A. F. Loureiro, "Malicious node detection in wireless sensor networks", 18th International Parallel and Distributed Processing Symposium, Proceedings (2004), pp. 24–30

[16]. Savitha Devi.M, Dr. P. Thanga Raj, "A Proportional Learning on Sink, Warm Hole Attacks with Prevention Algorithms in Wireless Sensor Networks PLSWHA-WSN, IJIRCCE Vol.2, Issue 10, October 2014

[17]. Resmi R, Lima Johnson et al., "Sinkhole attack in Mint Route and Multi hop LQI: Launching, Detection-A Survey", International Journal of Advanced Research Trends in Engineering and Technology (IJARTET). Vol. II, Special Issue X, March 2015

[18]. Noble George, Sujitha M., "Truthful Detection of Packet DroppingAttack in MANET", International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015

[19]. Md. Ibrahim Abdullah, Mohammad Muntasir Rahman et al., "Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count", I. J. Computer Network and Information Security, 2015, 3, 50-56

[20]. G. Keerthana, Dr. G. Padmavathi, "A Study on Sinkhole Attack Detection using SwarmIntelligence Techniques for Wireless Sensor Networks", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555

[21]. Fang-Jiao Zhanga B., Li-Dong Zhai et al., "Sinkhole attack detection based on redundancy mechanism in wireless sensor networks", Elsevier 2014 711-720

[22]. Rashmi Gupta et al., "Secured and Intelligent Multipath Routing Approach using AOMDV in MANET", IJCSMC, Vol. 5, Issue. 1, January 2016, pg.327 – 333