Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

How to Detect and Mitigate Sinkhole Attack in Wireless Sensor Network (WSN)

Abdulmalik Danmallam Bello
Dept. of Electronics and Communication Engineering,
Gyan Vihar School of Engneering Technology,
Suresh Gyan Vihar University Jaipur,
Rajasthan, India.

Dr. O. S. Lamba
Dept. of Electronics and Communication Engineering,
Gyan Vihar School of Engneering Technology,
Suresh Gyan Vihar University Jaipur,
Rajasthan, India

***Abstract*:- Wireless Sensor Network (WSN) is an emerging technology due to its wide range of applications in public and military area. These sensor networks consist of thousands of diminutive sensor nodes with limited resources with a base station of low cost and low power sensor nodes that are used for the monitoring purpose. Due to their energy limitations and positioning in hostile environments, WSNs are vulnerable to various routing attacks. Data authenticity, confidentiality, Integrity, and availability are the important security goals of WSNs.**

Most renowned attacks in WSN are Sybil attack, Denial of Service attack, wormhole attack, selective attack, HELLO Flooding attack, Sinkhole attack etc. Sinkhole attack is one of the most serious routing attacks because it attracts surrounding nodes with misleading routing path information and performs selective forwarding of data. Sinkhole attack is the kind of attack which degrades the performance of the network. It can cause an energy drain on surrounding nodes because it cause inappropriate and potentially dangerous responses based on false measurement.

The aim of this Research is to detect sinkhole attack in wireless sensor network and propose technique to fostall the attack and secure the network.

CHAPTER 1
INTRODUCTION

1.1 Introduction

Wireless Sensor Network (WSN) consists of large number of low-cost, resource-constrained sensor nodes with the ability to sense information from the sorrounding. The constraints of the wireless sensor node include low memory, low computation power, they are deployed in hostile area and left unattended, small range of communication capability and low energy capabilities. These characteristics makes this network vulnerable to several attacks, such as sinkhole attack. Sinkhole attack is a type of attack wehere compromised node tries to attract network traffic by advertising its fake routing update. One of the impacts of sinkhole attack is that, it can be used to launch other attacks like selective forwarding attack, acknowledge spoofing attack and drops or altered routing information.

Generally wireless sensor networks rely on many-to-one communication approach for data gathering. This approach is extremely susceptible to sinkhole attack, where an intruder attracts surrounding nodes with unfaithful routing information, and subsequently presents selective forwarding of data. Sinkhole attack is among the most destructive routing attack. It causes an important threat to sensor networks and it should be considered that the sensor nodes are mostly spread out in open areas and of weak computation and battery power. It can cause an energy drain on surrounding nodes and inappropriate and potentially dangerous responses based on false measurements.

Wireless Sensor Network is a collection of small devices which provides the ability to operate devices such as actuators, motors and switches that control conditions, and give reliable communication of sensed data. All the messages from sensor nodes in wireless sensor network are destined to base station. This created opportunity for sinkhole to launch an attack. Sinkhole attacks normally occur when compromised node send fake routing information to other nodes in the network with aim of attracting as many traffic as possible. Based on that communication pattern the intruder will only compromised the nodes which are close to base station instead of targeting all nodes in the network. This is considered as challenges because the communication pattern itself provides opportunity for attack.

1.2 Security in Wireless Sensor Network

Wireless sensor networks are usually installed in unsecured environments where security is the main issue and these networks are prone to attack. These networks are susceptible to many types of attacks.Because it is a large scale network it is not possible to monitor and protect each and every node. When the security is halted this network immediately response back with a message which requires sudden attention. Fake or tampered responses generated through the sensor nodes may lead to unwanted actions.

There are various security principles of wireless sensor network which are explained below:

Confidentiality: The transmission of data should be kept secret and not accessible to unauthorized user

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

Data Authentication: The unwanted affects can be avoided by ensuring the identity of the node with which it is communicating.

Integrity: It ensures the correctness of the data i.e. the data is not altered by the intruder.

Availability: The service should be accessible all the time.

Freshness: It suggests that data should be new no old data should be replayed.

Non-repudiation: It means that a node cannot deny sending a message which it has previously sent.

Authorization: It ensures that only authorized user can access to the resources of the network.

1.3 Related Work

Due to resource constraints traditional security mechanisms are not efficient for a WSN. Different researchers have proposed different solutions to detect and identify sinkhole attacks in wireless sensor networks. This section discusses these solutions.

Existing Approaches

The following are identified approaches by different researchers to detect and identified sinkhole attack in wireless sensor network. The approaches may be classified into anomaly based, rule based, statistical methods cryptographic key management, and hybrid systems.

Anomaly-based: in anomaly based detection normal user behavior is defined and the intrusion detection strategy is to search for anything that appears anomalous in the network. Rule based and statistical approaches are a subset of anomaly based detection approaches.

Rule based: In the rule based approach rules are designed based on the behavior or technique used to launch sinkhole attacks. These rules are implanted in intrusion detection system running on each sensor node or on specialized monitors. Any node will be considered an adversary and isolated from the network if it violates the rules.

Statistical: In statistical approaches data associated with certain activities of the nodes in network is recorded. For example, the network could monitor the normal packet transmission between the nodes or monitor resource depletion of the nodes such as CPU usage. Then the adversary or compromised node is detected by comparing the actual behavior with the threshold value which used as reference, any node exceeding that value is considered an intruder.

Cryptographic

In this approach the integrity and authenticity of packets traveling within the network is protected by using encryption and decryption keys. Any packet transmitted in the network is encrypted such that to access that message requires a key and any small modification of the message can be easily detected.

Hybrid

The combination of both anomaly and cryptographic approaches is used in this approach. The false positive rate produced by anomaly based methods is reduced in this approach due to the use of both methods. Another advantage of this approach is being able to catch any suspicious nodes when their signature is not included in detection database.

Rule Based Approaches

Krontiris et al. have developed distributed rule based systems to detect sinkholes. Their system runs on all individual sensor nodes. A collaborative approach can then used to identify and exclude the sinkhole.

Tumrongwittayapak and Varakulsiripunth proposed a system that uses the RSSI (Received Signal Strength Indicator) value with the help of extra monitor (EM) nodes to detect sinkhole attacks. One of their functions is to calculate the RSSI of nodes sending packets and send it to base station with the ID of source and next hop when nodes are deployed. The base station uses that value to calculate a VGM (visual geographical map). Later when the EM sends updated RSSI values and the base station identifies a change in packet flow from previous data a sinkhole attack can be detected

Sheela, Kumar and Mahadevan proposed a non-cryptographic method using mobile agents to defend against sinkhole attack. The mobile agents create an information matrix of each node by analyzing data transfer. Those information matrixes prevent wireless sensor nodes from believing the false path from sinkhole node.

Roy et al. proposed a Dynamic Trust Management system to detect and eliminate multiple attacks such as sinkhole attacks. Each node calculates the trust of its neighbor node based on experience of interaction; recommendation and knowledge then sends it to the base station. The base station decides which node is a sinkhole after it receives several trust values from other nodes.

Statistical Approaches:

Ngai, Liu and Lyu proposed a statistically based intruder detection algorithm to protect against sinkhole attacks in wireless sensor networks. Their algorithm involves the base station in the detection process. The results show the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

accuracy rate is good and the method has low communication overhead

Chen, Song and Hsieh proposed a GRSh (Girshick-Rubin-Shyriaev)–based algorithm, essentially a statistical algorithm, for detecting compromised nodes in wireless sensor networks. In this solution the data associated with certain resources or activities of the nodes are collected and analyzed. Then that value (threshold) is established and used as a reference to detect a malicious or compromised node in the network.

Cryptographic Approaches:

Sharmila and Umamaheswari proposed a message digest algorithm using cryptography to detect sinkhole attacks. In this system the sinkhole node is detected using an authentication key. When a node advertises new path information the node receiving it creates a digest of the message and sends it both via the original path and the path containing the suspect node. If the new node compromises the message the digest will be incorrect.

Papadimitriou et al. proposed two protocols, RESIST-0 and RESIST-1, that use a cryptographic approach in routing protocols to address the problem of sinkhole attacks. All authentication activity and signing of data message are done using public and private keys pre-established before the network is deployed

Hybrid Approaches:

Coppolino and Spagnuolo proposed a Hybrid Intrusion detection system to detect sinkhole and sleep deprivation attacks. The proposed system combines anomaly and signature-based detection. Detection of anomalous behavior is used to insert suspicious nodes on a blacklist after analyzing the collected data from neighbors.

1.4 Review of Literature

Abdullah et al. (2015) proposed sinkhole detection using hop counting technique. The proposed technique can detect successfully when the malicious nodes are situated at distant from base station where it reports with less accurately when malicious node are located near the base station.

Patel et al. (2016) detected sinkhole attack based on the analysis of routing behaviour in a wireless sensor network. The proposed algorithm consists of three phases namely, topology generation & data transmission, sinkhole implementation and detection phase. By analysing the forward and reverse routes this scheme detects the sinkholes.

Mathew et al. (2017) discovered and examined the existing solutions which are employed for detection of sinkhole attack in wireless sensor network. They focused on techniques viz., cryptography, sequence number, hop count and mobile agent. They found that mainly techniques have security issues, high communication cost, low detection rate and high detection overheads.

Sehrawat et al. (2018) [55] analyzed the impact of Sinkhole attack on AODV protocol with varying number of attacker nodes. Simulated the proposed methodology in Qualnet 7.3.1 software using 50 nodes in an area of 1500 m x 1500 m with no mobility. Result showed low throughput, increase in packet drop, increase in RREP messages with increase in malicious nodes.

CHAPTER 2
SINKHOLE ATTACK

2.1 Sinkhole Attack

Sinkhole attack is an attack were an intruder compromise a node inside the network and launches an attack. Then the compromise node try to attract all the traffic from neighbor nodes based on the routing metric that used in routing protocol. When it managed to achieve that, it will launch an attack. Due to communication pattern of wireless sensor network of many to one communication where each node send data to base station, makes this WSN vulnerable to sinkhole attack.

Sinkhole attacks are a type of network layer attack where the compromised node sends fake routing information to its neighbors to attract network traffic to itself. Due to the ad hoc network and many to one communication pattern of wireless sensor networks where many nodes send data to a single base station, WSNs are particularly vulnerable to sinkhole attacks. Based on the communication flow in the WSN the sinkhole does not need to target all the nodes in the network but only those close to the base station.

In this attack the traffic is attracted by the hostile node. The hostile node draws consideration of their neighboring nodes by reporting a fake ideal way by utilizing appealing force or data transfer capacity. Tricked neighboring nodes then course their information to hostile/malicious node and results packet dropping by the malicious node. Many attacks like eavesdropping, selective forwarding and black holes, etc. can be empowered by Sinkhole attack.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

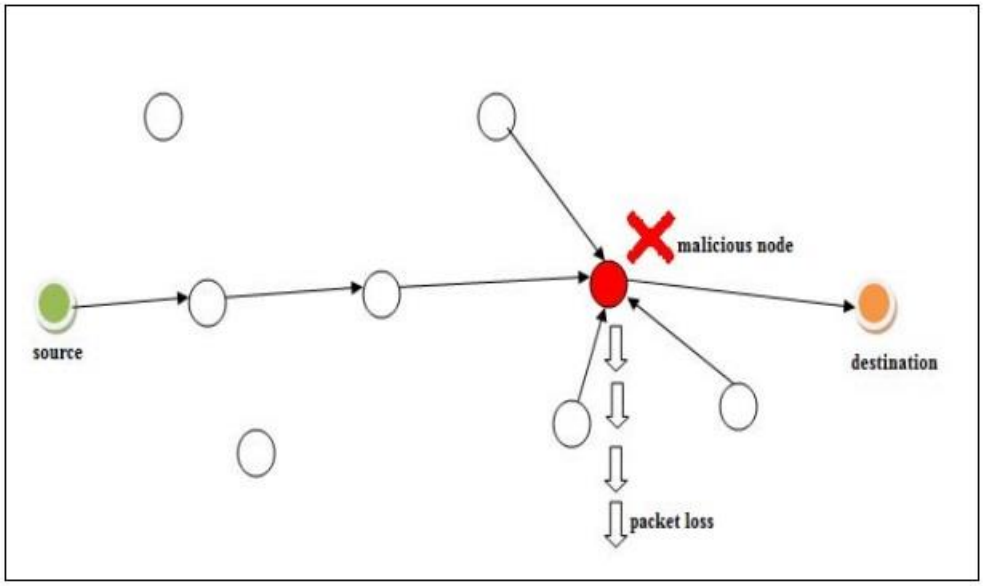


Fig. 1 Sinkhole Attack in WSN Sinkhole Attack In WSN

The figure above represents the diagrammatic view of sinkhole which lures the entire surrounding traffic local to the malicious node that path through malicious node is optimum. With all the surrounding nodes sending data packets to the malicious nodes thus creates a sinkhole at the center. The traffic from the source node is dropped by the malicious node as shown in the diagram.

We consider two scenarios of sinkhole attacks. In the first the intruder has more power than other nodes. In the second the intruder and other nodes have the same power. In both cases the intruder claims to have the shortest path to base station so that it can attract network traffic. In a wireless sensor network the best path to the base station is the basic metric for routing data

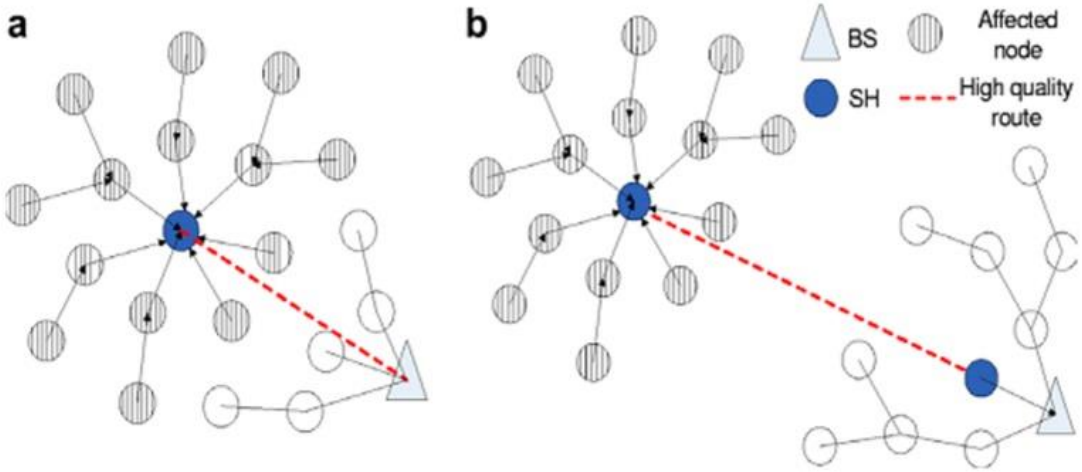


Fig. 2 Two illustrations of sinkhole attack in WSN

a) using artificial high quality rout
b) using worm hole

a) The intruder has greater computational and communication power than other nodes and has managed to create a high quality single hop connection with the base station. It then advertises its high quality routing message to its neighbors. After that all the neighbors will divert their traffic to the base station to pass through the intruder and the sinkhole attack is launched.

b) The sinkhole attack is launched in conjunction with a wormhole attack. This attack involves two compromised nodes linked via a tunnel or wormhole

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

TABLE 1 Attacks on Different Layers in Wireless Sensor Networks And Dos Defenses

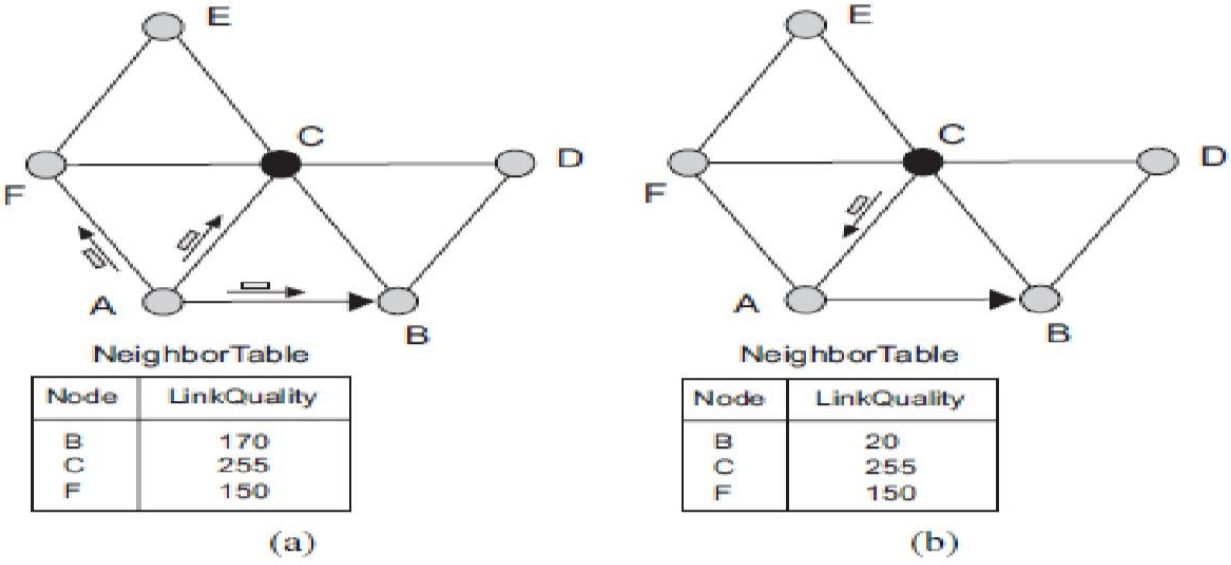
Layer	Attack	Denial-of-Service Defense
Transport Layer	Flooding, Desynchronization	Client puzzles, Authentication
Network Layer	Routing Attacks like black hole, Sinkhole, Wormhole etc.	Authorization and Monitoring
Data link layer	Collision, Exhaustion, Unfairness	Error-correction code, Rate limitation, Small frames
Physical layer	Jamming Attack, Tempering	Spread spectrum, priority messages, region mapping

From the above table Sinkhole attack is activated at the network layer. Due to this attack the performance and efficiency of the network decrease and packet loss increase

2.2 The following subsections discuss the techniques use in MintRoute protocol and AODV protocol in launching sinkhole attack.

Sinkhole Attack in MintRoute Protocol

MintRoute protocol is a type of protocol which is commonly used in wireless sensor network. It was designed purposely for the wireless sensor network, it is light and suitable for sensor nodes which have minimum storage capacity, low computation power and limited power supply. MintRoute protocol uses link quality as a metric to choose the best route to send packet to the Base Station



Gig. 3 Sinkhole attack in MintRoute protocol (Krontiris)

MintRoute protocol is a type of protocol which is commonly used in wireless sensor network. It was designed purposely for the wireless sensor network, it is light and suitable for sensor nodes which have minimum storage capacity, low computation power and limited power supply. MintRoute protocol uses link quality as a metric to choose the best route to send packet to the Base Station (Krontiris et al [15]).

Fig. 3 above shows six sensor nodes A, B, C, D, E, and F. Node C is malicious, and it is going to launch a sinkhole attack. The Figure

(a) shows a route table of node A with IDs of its neighbors with their corresponding link quality. Originally the parent node was node B but node C advertises its link quality with a value of 255 which is maximum value. Node A is not going to change its parent node until the node B's link quality fall to 25 below the absolute value.

(b) the malicious node is sending new update route packet that the link quality fall up to 20 and impersonate node B so that node A believe the packet come from node B. Node A will update its route table and change the parent node to node C (Krontiris et al [15]). The attacker uses node impersonation to launch an attack.

Sinkhole Attack in TinyAODV Protocol This is another explanation of sinkhole attack in wireless sensor network and this time the attack is launched under TinyAODV (Ad-hoc On Demand Vector) protocol. TinyAODV protocol is the same as AODV in MANET but this one is lighter compared to AODV and it was modified purposely for wireless sensor network. The number of hops to base station is the routing metric that used in this protocol. Generally the route from source to destination is created when one of the nodes send a request, the source node sends a RREQ (Route request) packet to his neighbors when wants to send packet. Next one of the neighbors close to destination is reply by sending back RREP (Route Reply) packet, if not the packet is forwarded to other nodes close to that destination. Finally, the source receives RREP packet from neighbor then select one node with less number of hops to destination. The sinkhole node or compromised node launches an attack by send back RREP packet. In RREP packet it gives small number of hops which indicates close proximity to the base station. Then the source node decides to forward packet to sinkhole node. The compromised node then performs the same technique to its entire neighbors and tries to attract as much

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

traffic as possible. For instance, Fig below shows node M launches sinkhole attack in Tiny AODV. Node A sends RREQ to nodes BCM. However node M instead of broadcast to node E like nodes B and C does to node D, he replies back RREP to node A. Then node A will reject node B and C, then forward packet to M because node A and B are very far to F compare to node M.

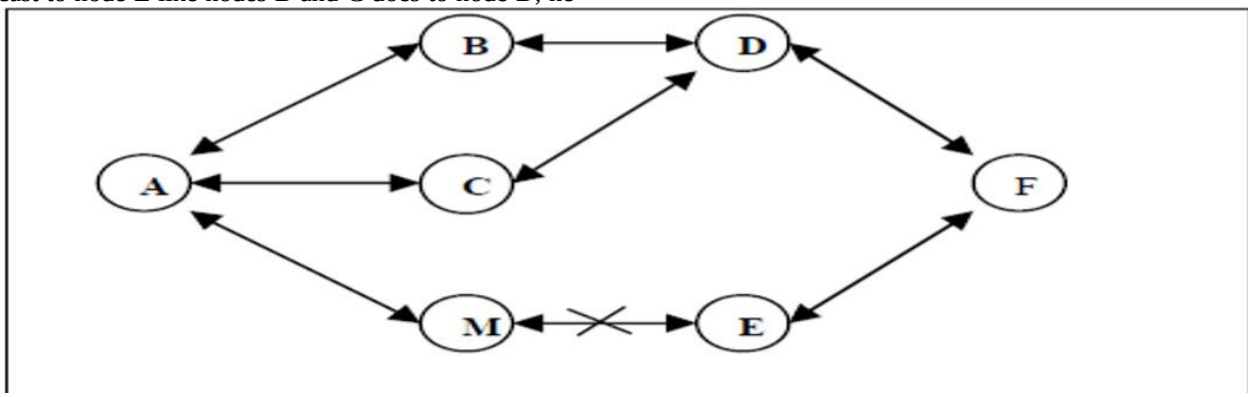


Fig. 4 Sinkhole in TinyAODV protocol (Teng and Zhang)

2.2 Challenges in Detection Of Sinkhole Attack in WSNs

The following are the main challenges in detecting sinkhole attack in wireless sensor

Communication Pattern in WSN; All the messages from sensor nodes in wireless sensor network are destined to base station. This created opportunity for sinkhole to launch an attack. Sinkhole attacks normally occur when compromised node send fake routing information to other nodes in the network with aim of attracting as many traffic as possible. Based on that communication pattern the intruder will only compromised the nodes which are close to base station instead of targeting all nodes in the network. This is considered as challenges because the communication pattern itself provides opportunity for attack.

Sinkhole attack is unpredictable; In wireless sensor network the packet are transmitted based on routing metric that used by different routing protocols [26]. The compromised node used its routing metric that used by routing protocol to lie to his neighbors in order to launch sinkhole attack. Then all the data from his neighbors to base station will pass through compromised node. For example the techniques used by compromised node in network that used TinyAODV protocol is different to the one used another protocol like MintRoute protocol. In MintRoute they used link quality as route metric while in Tiny AODV they used number of hop to base station as routing metric. Therefore the sinkhole attack techniques is changed based on routing metric of routing protocol

Insider Attack Insider attack and outsider attack are two categories of attack in wireless sensor network. Outside attack is when intruder is not part of network. In inside attack the intruder compromises one of the legitimate node through node tempering or through weakness in its system software then compromised node inject false information in network after listen to secret information. Inside attack can disrupt the network by modifying routing packet. Through compromised node sinkhole attack attract nearly all the traffic from particular area after making that compromised node attractive to other nodes. The fact is that compromised node possesses adequate access privilege in the network and has knowledge pertaining to valuable information about the network topology this created challenges in detecting. Base to that situation even cryptographic cannot defend against insider attack although it provides integrity, confidentiality and authentication. Therefore the internal attack has more serious impact on victim system compared to outsider attack.

Resource Constraints; The limited power supply, low communication range, low memory capacity and low computational power are the main constrained in wireless sensor network that hinder implementation of strong security mechanism. For example the strong cryptographic method that used in other network cannot be implemented in this network due to low computational power and low memory capacity. Therefore less strong key are considered which is compatible with available resources.

Physical attack; A wireless sensor network normally deployed in hostile environment and left unattended. This provides a opportunity for an intruder to attack a node physically and get access to all necessary information

CHAPTER 3
DETECTION AND MITIGATION APPROACH

3.1Detection and Mitigation Approach

In this research work Delphi (Delay per Hop Indicator) technique is propose technique use to solve the problem. The advantage of Delphi is that it does not require clock synchronization and position information and it does not require the mobile nodes to be equipped with some special hardware, which in turn provide higher power efficiency. The Disadvantage of Delphi method is it cannot pinpoint the malicious node location. This disadvantage of Delphi method can be overcome by using Geographical Detection. The proposed Solution is elaborated as follows

wireless sensor network is deployed in a fixed area and with the fixed number of nodes; the network deployed is decentralized in nature.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

• After deploying the wireless sensor network the path from the source to the destination was established with the help of the AODV routing protocol.

• The source node floods the route request packets in the network for the path establishment to the destination and the adjacent nodes of the destination will reply back to the source node with the route reply packets

• After the route request packets and the route reply packets, the best path is selected from the multiple paths for sending the packets from the source to the destination.

• The malicious node existing in the path which will trigger sinkhole attack and is responsible to change the delay between the source and destination.

• By calculating the delay per hop for each node existing in the path the presence of the malicious node is detected.

• The neighbor of each node in the network and its distance from the source node traced. This helps to find out the location of the node responsible for the sinkhole attack
• Then the malicious node is removed from the network and new path is formed from the source to the destination to send the data packets.

3.2 ALGORITHM

1. Deploy wireless sensor network with finite number of sensor network
2. The source and destination nodes are defined in the network
3. The source send route request packets in the network to establish path to destination
4. On the basis of hop count and sequence number shortest path will be established from source to destination
5. Delay per hop will be calculated in the network.
6. If (delay< defined delay)
7. Calculate Euclidian distance of each node
8. Using the ping point technique of Delphi detect malicious node from the network and isolate from the network
9. Else
10. Source continue from source to destination

CHAPTER 4
CONCLUSION

Conclusion

1. Packet Loss: It is a phenomenon in which a packet traveling from a source fails to reach destination. When the attack is isolated from the network packet loss will be reduced.
2. Throughput: Throughput is the average rate of packets which are successfully delivered over communication channel. When the attack is isolated from the network throughput will be increased.
3. Delay: It is average time taken by data packets to reach destination. In this technique the delay in the attacked scenario will be increased while delay in the new scenario will be reduced

REFERENCE

[1] J. Qi, T. Hong, K. Xiaohui, and L. Qiang, “Detection and defence of Sinkhole attack in Wireless Sensor Network” in Communication Technology (ICCT), 2012 IEEE 14th International Conference on, 2012, pp. 809-813.
[2] D. G. Padmavathi and M. Shanmugapriya, “A survey of attacks, security mechanisms and challenges in wireless sensor networks” arXiv preprint arXiv:0909.0576, 2009.
[3] H. Modares, R. Salleh, and A. Moravejosharieh, “Overview of security issues in wireless sensor networks” in 2011 Third International Conference on Computational Intelligence, Modelling & Simulation, 2011, pp.308-311.
[4] C. Chen, M. Song, and G. Hsieh,”Intrusion detection of sinkhole attacks in large-scale wireless sensor networks” in Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on, 2010, pp. 711-716.
[5] N. Gandhewar and R. Patel, “Detection and Prevention of sinkhole attack on AODV Protocol in Mobile Adhoc Network” in Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on, 2012, pp. 714-718.
[6] Y. Zhou, Y. Fang, and Y. Zhang, “Securing wireless sensor networks: a survey” IEEE Communications Surveys & Tutorials, vol. 10, pp. 6-28, 2008.
[7] Amrita Ghosal and Subir Halder, “Intrusion Detection in Wireless Sensor Networks: Issues, Challenges and Approaches”, Wireless Networks and Security (2013): 329-367.
[8] Robert Mitchell and Ing-Ray Chen, “A survey of intrusion detection in wireless network applications”, Computer Communications 42 (2014): 1-23.
[9] Ioannis Krontiris, Tassos Dimitriou, Thanassis Giannetsos, and Marios Mpasoukos , “Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks”, ALGOSENSORS (2007):150-16.
[10] Ashfaq Hussain Farooqi and Farrukh Aslam Khan, “Intrusion Detection Systems for Wireless Sensor Networks: A Survey”, FGCN/ACN 56 (2009): 234-241.
[11] Abhishek Pandey and R.C. Tripathi. (2010). A Survey on Wireless Sensor Networks Security, International Journal of Computer Applications (0975 – 8887) Volume 3 – No.2.
[12] Changlong Chen, Min Song, and George Hsieh (2010) Intrusion detection of Sinkhole attack in large scale Wireless Sensor Networks, In Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on (pp.711-716).IEEE
[13] Chen, C., Song, M. and Hsieh, G. (2010). Intrusion Detection sinkhole attack in large scale wireless sensor network, In Wireless Communication, Networking and Information Security (WCNIS), 2010 IEEE Interational Conference on (pp. 711-716). IEEE.
[14] Choi, G. B., Cho, J. E., Kim,H. J., Hong, S. C. and Kim, H. J. (2008).A sinkhole attack detection mechanism for LQI based mesh routing in WSN. In ICOIN (pp.1-5).
[15] Chun-ming Rong , Skjalg Eggen, Hong-bing Cheng. (2011). A Novel Intrusion Detection Algorithm for Wireless Sensor networks. In Wireless Communication, Vehicular Technology, information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on (pp. 1-7).
[16] Coppolino, L., D’Antonio, S., Romano, L., and Spagnuolo, G.(2010). An intrusion detection system for critical information infrastructures using WSN technologies. In Critical Infrastructure (CRIS), 2010 5th International Conference on (pp. 1-8). IEEE
[17] Daniel Dallas, Christopher Leckie, Kotagiri Ramamohanarao. (2007). Hop-Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks, In Networks, 2007. ICON 2007. 15th IEEE International Conference on (pp. 176-181)
[18] David Martins and Hervé Guyennet. (2010) Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey, In Network-Based Information Systems (NBiS), 2010 13th International Conference on (pp. 313320). IEEE
[19] Edith C. H. Ngai, Jiangchuan Liu and Michael R. Lyu. (2006). On the Intruder Detection for Sinkhole Attack in Wireless Sensor

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

Networks, In Communications, 2006. ICC'06. IEEE International Conference on (Vol.8, pp. 3383-3389). IEEE.

[20] Fessant, F., Papadimitriou, A., Viana, A.,Sengul, C. and Polamar, E. (2011) A sinkhole resilient protocol for wireless sensor network: Performance and security analysis. Computer Communications, 35(2), 234-248.

[21] G.H. Raghunandan, B.N. Lakshmi. (2011.). A Comparative Analysis of Routing Techniques for Wireless Sensor Networks, In Innovations in Emerging Technology (NCOIET), 2011 National Conference on (pp. 17-22). IEEE

[22] Jaydip Sen. (2009). A Survey on Wireless Sensor Network Security, International Journal of Communication Networks & Information Security, 1(2).

[23] Kalpana Sharma and M K Ghose. (2010) Wireless Sensor Networks: An Overview on its Security Threats, IJCA, Special Issue on "Mobile Ad-Hoc Networks" MANET.

[24] Krontiris,I., Dimitriou,T., Giannetsos,T. and Mpasoukos, M. (2008). Intrusion Detection Sinkhole Attacks in Wireless Sensor Network. In Networking and Communications, 2008. WIMOB'08. IEEE Interational Conference on Wireless and Mobile Computing, (pp. 526-531). IEEE.

[25] Krontiris, I., Giannetsos, T. and Dimitriou, T. (2008). Launch Sinkhole Attack in Wireless Sensor Network; the Intruder Side. In Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing, (pp. 526-531). IEEE.

[26] Krontiris, I. Dimitrou, T. Freiling, F.C. (2007). Towards intrusion detection in wireless sensor networks. In Proc. Of the 13th European Wireless Conference.

[27] Liping Teng and Yongping Zhang. (2010). SeRA: A Secure Routing Algorithm against Sinkhole Attacks for Mobile Wireless Sensor Networks, In Computer Modelling and Simulation, 2010. ICCMS'10. Second International Conference on (Vol. 4, pp. 79-82).

[28] Ngai, E., Liu, J and Lyu, M. (2007) An efficient intruder detection algorithm against sinkhole attack in wireless sensor network. Computer Communications, 30(11), 2353-2364.

[29] Ngai, E., Liu, J. and Lyu, M. (2006). On intruder detection for Sinkhole attack in Wireless Sensor Network. In Communications, 2006. ICC'06.IEEE International Conference on (Vol. 8, pp.3383-3389). IEEE

[30] P. Samundiswary, D.Sathian and P. Dananjayan. (2010). Secured greedy perimeter stateless routing for wireless sensor networks, International Journal of Ad hoc, Sensor & Ubiquitous Computing(IJASUC)1, (2)

[31] Papadimitriou, A., Fessant, L. F. and Sengul, C. (2009). Cryptographic protocols to fight sinkhole attacks on tree based routing in WSN. In Secure Network Protocols, 2009. NPSec 2009. 5th IEEE Workshop on (pp.43-48). IEEE

[32] Pathan, K., AI-S. (2011) Security of SelfOrganizing Networks-MANET, WSN, VANET, WMN. ISB N-13:978-1-4398-1920-3. Taylor and Francis Group.

[33] Roy, D.S., Singh, A.S. and Choudhury, S. (2008). Countering Sinkhole and Blackhole Attacks on Sensor Networks using Dynamic Trust Management. In Computers and Communications, 2008. ISCC 2008. IEE Symposium on (pp. 537-542). IEEE.

[34] Sharmila, S. and Umamaheswari, G. (2011). Detection of sinkhole attack in WSN using message digest algorithms. In Process Automation, Control and Computing (PACC), 2011 International Conference on (pp. 1-6). IEEE.

[35] Sheela, D., Kumar, N., and C Dr. Mahadevan, G.C.(2011). A non-Cryptographic Method of Sinkhole Attack Detection in Wireless Sensor Networks. In Recent Trends in Information Technology (ICRTIT), 2011 International Conference on (pp.527-532). IEEE

[36] Suman Deb Roy, Sneha Aman Singh, Subhrabrata Choudhury, and N. C. Debnath. (2008). Countering Sinkhole and Black hole Attacks on Sensor Networks J. young Kim, R. D. Caytiles, and K. J. Kim "A review of the vulnerabilities and attacks for wireless sensor networks" Journal of Security Engineering, 2012.

[37] A.-S. K. Pathan, H.-W. Lee, and C. S. Hong,"Security in wireless sensor networks: issues and challenges" in 2006 8th International Conference Advanced Communication Technology, 2006, pp. 6 pp.-1048.

[38] E. C. Ngai, J. Liu, and M. R. Lyu, "On the intruder detection for sinkhole attack in wireless sensor networks" in 2006 IEEE International Conference on Communications, 2006, pp. 33833389.

[39] Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala, " Detection of sink hole Attack in wireless sensor networks",IEEE International Conference on Space Science and Communication, July 2013, pp. 361-365.