SINKHOLE ATTACK IN WIRELESS SENSOR

Neha Thakur[1], Asst Prof. Mrs Prachi Shahare[2]
[1]M.Tech-CSE IV Semester (Multimedia Technology),
Department of Computer Science & Engineering, Kalinga University, Naya Raipur (C.G)

ABSTRACT: In this paper we investigate in depth one of the most severe attacks against sensor networks such as selective forwarding, jamming, sinkhole, wormhole etc. Sinkhole attack is the major common internal attack for these networks and we are proposing a detection system for identifying sinkhole attacks in Wireless Sensor Networks (WSN). Unattended installation of sensor nodes in the environment causes many security threats in the wireless sensor networks on WSNs. These attacks are performed by creating a malicious node with the highest transmission range to the base station and ultimately this drop of some important data packets can disrupt the sensor networks completely. We have presented some countermeasures against the sinkhole attack. We have presented some countermeasures against the sinkhole attack.

I. INTRODUCTION

WSNs typically consist of small and inexpensive devices deployed in open, unprotected, and unattended environments for long term operations to monitor and collect data. This data is subsequently reported back to the base station over a wireless link. The WSN is vulnerable to various attacks; hence security is an important factor and what makes it even easier for attackers is the fact that most protocols for sensor networks are not designed having security threats in mind. As a consequence, deployments of sensor networks rarely include security protection and little or no effort is usually required from the side of the attacker to perform the attack. But securing sensor networks against these threats is also not that simple, the major factor is that the sensor nodes have limited memory, power, computational capability, and transmission range. the limited resources nature of sensor networks posts a great challenge to any proposed security solution so, it is very important to study realistic attacker models and evaluate the practicality and efficiency of certain attacks.This paper deals with the most impotent internal attack called sinkhole attack. In this type of attack, an attacker compromises an existing node in the network or brings a new external node, which has same capabilities of an existing node and uses this compromised node to create the sinkhole attack

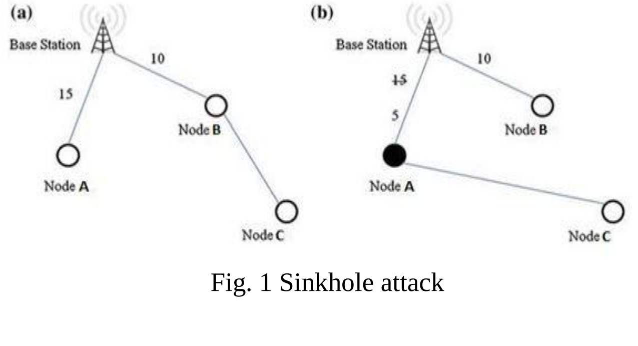

Fig. 1 Sinkhole attack

Figure 1a represents the sensor network demonstration prior to a sinkhole attack. If node C wants to communicate to the base station, it can send information only through node A or node B. In the above figure, node B can be selected as apparent to node id C because node id B has the shortest distance to the base station.

In Figure 1b Node A is the compromised node now; it announces that it has the shortest path to the base station to all of its neighbours. This reflects node C to change its parent and route the packets through node A to the base station .If the intruder succeeds in launching the sinkhole attack, then the compromised node will attract all the traffic from neighbouring nodes to choose this node as a parent node. For attracting the neighbouring nodes, the compromised node will use the cost metric of Mint- Route protocol. Sinkhole attacks are the network layer attacks. In this, the compromised node will broadcast false link quality information to all its surrounding nodes. In this paper we considered popular link quality-based multi-hop routing protocol named as Mint-Route protocol of Tiny OS . For the calculation of link quality, each and every node will periodically transmit the route update packet to all its neighbours. Intrusion detection is the process of discovering, analyzing, and reporting unauthorized activities in a network. Intrusion detection discovers violations of integrity, confidentiality, availability of data, and availability of resources in the network. Intrusion detection in WSNs is useful for identifying an intruder, an attacker who has gained control of a sensor node, or injected false data or recurring packets into the sensor network.

II. TYPES OF ATTACKS ON WIRELESS SENSOR NETWORKS

The Sensor networks are self-organizing networks which, once deployed, are expected to run autonomously and without human attendance.
Major attacks on sensor networks are as follow:

JAMMING

Jamming interferes with the radio frequencies of the sensor nodes. Only a few jamming nodes can put a considerable amount of the nodes out of order. If the adversary can block the entire network then that constitutes complete DoS.

TAMPERING

A tampering attacker may damage a sensor node, replace the entire node or part of its hardware or even electronically interrogate the nodes to gain access to sensitive information, such as shared cryptographic keys and how to access higher communication layers.

SPOFFED, ALTERED OR REPLAYED ROUTING INFORMATION

This is the most direct attack. By spoofing, altering or replaying routing information the attacker can complicate the network and create routing loops, attracting or repelling traffic, generating false error messages, shortening or extending source routes or partitioning the network.

SELECTIVE FORWARDING

In such an attack the adversary includes itself in a data flow path of interest. Then the attacker may choose not to forward certain packets and drop them causing a sort of black hole.

THE SYBIL ATTACK

A malicious node present multiple identities to the network is called Sybil attack. This attack is especially confusing to geographic routing protocols as the adversary appears to be in multiple locations at once.

WORMHOLES

In these attacks the adversary tunnels messages received in one part of the network over a low latency link, to another part of the network where the messages are then replayed. Wormholes often convince distant nodes that they are neighbours, leading to quick exhaustion of their energy resources. An attacker close to the base station can completely disrupt routing by creating well positioned wormholes that convince nodes multiple hops from the base station that they are only a couple of hops away through the wormhole.

HELLO FLOOD ATTACKS

In many routing protocols, nodes broadcast hello messages to announce their presence to their neighbours. A node receiving such a message can assume that the node that sent the message is within its range. An attacker with a high powered antenna can convince every node in the network that it is their neighbour.

III. SINKHOLE ATTACKS

In a sinkhole attack an intruder compromises a node or introduces a counterfeit node inside the network and uses it to launch an attack. The compromised node tries to attract all the traffic from neighbour nodes based on the routing metric used in the routing protocol. When the compromised node manages to achieve that, it will launch an attack. Sinkhole attacks are a type of network layer attack where the compromised node sends fake routing information to its neighbours 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. 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.

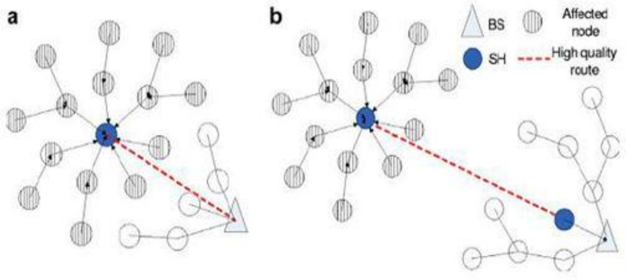

Fig. 2. Two illustrations of sinkhole attack in WSN a) using artificial high quality route b) using

In figure 2(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 neighbours. After that all the neighbours will divert their traffic to the base station to pass through the intruder and the sinkhole attack is launched.

In Figure 2(b) the sinkhole attack is launched in conjunction with a wormhole attack. This attack involves two compromised nodes linked via a tunnel or wormhole.

IV. 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 APROACHES

We have identified the following approaches by different researchers to detect and identified sinkhole attack in wireless sensor network. Approaches taken by previous researchers 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 [9].

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 [10]. 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 behaviour 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. 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 [11] Another advantage of this approach is being able to catch any suspicious nodes when their signature is not included in detection database.

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 [11] Another advantage of this approach is being able to catch any suspicious nodes when their signature is not included in detection database.

V. SUMMARY OF PREVIOUS RESEARCH

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 Zpdated 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 neighbour 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 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: A Hybrid Intrusion detection system was proposed by Coppolino and Spagnuolo 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 neighbours.

VI. CONCLUSION

In contrast to traditional networks, Wireless Sensor networks (WSN) are more vulnerable to attacks. Amongst all major attacks on sensor networks, sinkhole attack is the most destructive routing ttacks for these networks. In this paper, we have surveyed various countermeasure techniques for sinkhole attack. Which approach to use depends on the particulars of the WSN in question. For example, a WSN where the sensor nodes are difficult to subvert and have sufficient power may be well served by a cryptographic approach although key distribution and initial authentication remains a significant problem. WSNs where new nodes are not added after initial setup may be well served by a rule based approach. Another significant challenge is application in real world WSNs beyond the laboratory. One interesting area for further research is avoiding sinkholes in ad hoc mesh networks where the devices are not specialized such as cell phone or wireless laptop networks.

REFERENCES

[1] Teng, L., Zhang, Y.: SeRA: A Secure Routing Algorithm Against Sinkhole Attacks for Mobile Wireless Sensor Networks. 2010 Second International Conference on Computer Modeling and Simulation. pp. 79–82. IEEE (2010).

[2] Sharma, K., Ghose, M.: Wireless sensor networks:

An overview on its security threats. Int. J. Comput. Their Appl. 42–45 (2010).

[3] Ngai, E.C.H., Liu, J., Lyu, M.: On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks. 2006 IEEE International Conference on Communications. pp. 3383–3389. IEEE,

[4] D.Sheela, Naveen kumar. C and Dr. G.Mahadevan; "A Non Cryptographic Method of Sinkhole Attack Detection in Wireless Sensor Networks" IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011, pp. 527-532

[5] Levis, P., Madden, S., Polastre, J., et al.: TinyOS: an operating system for sensor networks. Springer, Berlin Heidelberg (2005)

[6] Pahlavan, K., Li, X.: Indoor geo-location science and technology. IEEE Commun. Mag. 40(2), 112–118 (2002)

[7] Umashri, K., Dr. Nalini, N.: Detecting sinkhole attack in wireless sensor networks. Int. J. Scient. Eng. Res. 5, 6, (2014)

[8] Edith C. H. Ngai, Jiangchuan Liu and Michael R. Lyu; "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks" IEEE International Conference on Communications, 2006,Volume 8, pp. 3383-3389.

[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] Chanatip Tumrongwittayapak and Ruttikorn Varakulsiripunth; "Detecting Sinkhole Attacks in Wireless Sensor Networks" ICROS-SICE International Joint Conference 2009, pp. 1966-1971.

[11] Changlong Chen, Min Song, and George Hsieh; "Intrusion Detection of Sinkhole Attacks In Large-scale Wireless Sensor Networks" IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), 2010, pp. 711-716.