RESEARCH ARTICLE OPEN ACCESS

A Survey on Wormhole and Sinkhole Attack Detection and Prevention Techniques in Manet

D.Sasirekha*, Dr.N.Radha**
**(Research Scholar, Department of Computer Science, PSGR krishnammal college for women, Coimbatore, India*
Email: rekha2131994@gmail.com)
*** (Assistant Professor, Department of Computer Science, PSGR Krishnammal college for women, Coimbatore, India)*

ABSTRACT
Nowadays with the wide range of applications in wireless networks, there is an increasing need for security of these networks. Specifically, the Mobile Ad-hoc networks are very easy to vulnerable due to many security threats and attacks. These networks have been subjected to numerous attacks among which Sinkhole and wormhole attack are the prominent attacks. In the network routing these attacks should be identified earlier and recovered soon. In the wormhole attack, the data transferred to more routes or the malicious node abused the received data into many ways. In the Sinkhole attack the attacker seeks the data transferred by attracting the node in various ways. Various solutions are found to detect these network attacks. In this paper, a comparative analysis of those techniques is performed. This study finds the impact and suitable methods to prevent and detect wormhole and sinkhole attacks in Mobile ad-hoc networks.

Keywords - MANET, Network security, Sinkhole attack, Wormhole attack.

Date of Submission: 09-11-2017 Date of acceptance: 28-11-2017

I. INTRODUCTION

A mobile ad hoc network (MANET) is a mobile device which can communicate with each other without the use of a pre-defined infrastructure. MANET has high mobility and it doesn't rely on the previous network infrastructure. It has huge dynamic topological structure. This flexible nature of MANET always creates many security issues and vulnerabilities. In case of infrastructure based computer network, attackers either requires to physically access the network, or violate multiple security mechanisms similar to firewall or gateway in order to carry out any attack on the target device. However, in MANET, it is not essential for the attacker to physically access the network. At any time, if the attacker locations itself within communication range of other node in the mobile network, it can establish communication with that node and join the MANET. Hence, MANET does not possess any secure boundary for defending themselves from possibly hazardous network accesses. Missing of these secure boundaries exposes the MANET to be vulnerable to attacks. Many researches were described the importance of MANET security with reliable proactive and reactive routing protocols. Due to the lack of server oriented process and centralized authority process, the MANET affected by the Black hole, Gray hole and many attacks. So, deploying appropriate solution for such attacks was the most concentrated research approach. In MANET the Mobile nodes can join or leave the network easily. Hence, it is difficult for the nodes to prevent such attacks by the nodes it communicates with. Due to the flexibility in network topology and high mobility of the nodes in the ad hoc network, a compromised node can frequently change its attack target and perform malicious behavior to other mobile node in the network. It is very difficult to track the malicious behavior of a compromised node. This survey brings the outline and conclusion of many previous approaches on wormhole and sinkhole attacks.

II. LITERATURE REVIEW

Mobile Ad-hoc Networks are distressed by many attacks; the major two categories are active and passive attacks. In this survey, detection and prevention techniques of two network layer attack is studied. One is wormhole attack and another one is sinkhole attack.

Wormhole attack detection and prevention techniques:

Wormhole attacks are very difficult to detect, as they are launched by two or more nodes in collaboration with each other and they work in two phases. In the first phase, malicious nodes try to convince legitimate nodes to transfer data through them in order to get access to more routes. In the second phase, malicious nodes exploit the received data in a variety of ways. In the wormhole attack an adversary or malicious node tunnels messages received in one part of the network over a low-latency link and replays them in a different part of the network through a private channel. Route between source node and destination node is selected through the private channel due to the less number of hops or less time, as compared to packets send out over other normal routes. An adversary or malicious nodes situated close to a base station can be able to completely interrupt routing by forming well-placed wormhole nodes A1 and A2. The Node node1 sending the packets may reach the destination node node6 via both routes, which are normal route (node1–node2–node3–node4–node5–node6) and route, formed by wormhole nodes A1 and A2 shown in fig 1.

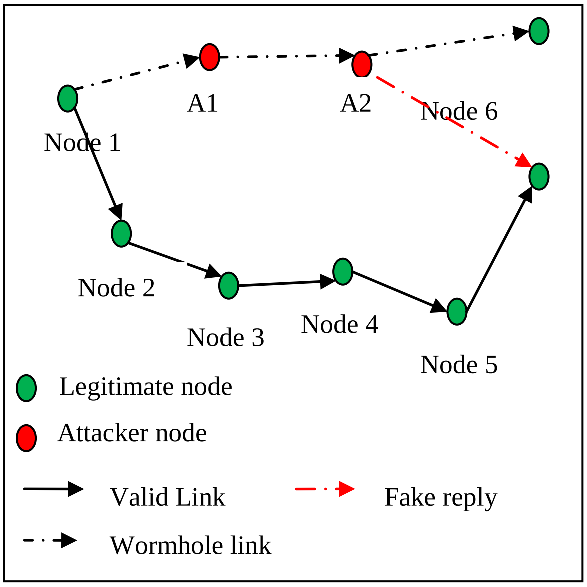

Fig 1. Wormhole attack scenario

The packets that follow the normal route, i.e. node1–node2–node3–node4–node5–node6, reach destination node node6 later than those transferred through the wormhole and are therefore dropped because normal route do more hops. Therefore, the wormhole nodes attracting the packets by forming false routing between source and destinations and the packets tunneled by wormhole nodes can be drop, modify, or send data to a third party for malicious purposes. Wormholes are hard to detect and can strongly influence on the performance of network services such as localization, data fusion and time synchronization. This attack also forms a serious threat in wireless networks, especially against routing protocols. Several researchers have proposed different solutions to deal with wormhole attacks. Most of the solutions are time-based, statistical, or neighborhood-based solutions.

DB. Johnson et al., [1] introduced the temporal leash approach. Leash is additional information attached with the packet, which contains geographical and temporal messages. In this paper, author proved the graphic leashes are less efficient than temporal leashes. This requires authentication on every broadcast. This is most reliable to the network when the time synchronization is indistinct.

Maulik et al., [2] analyzed the performance of MANET with the wormhole attack scenario. Authors considered the many QoS parameters such as delay, throughput, packet delivery ratio (PDR), node energy (NE), and node density etc. these QOS parameters were tested using NS2 simulator. The authors utilized the Reference Point Group Mobility Model (RPGM) to study node density effect and initial energy on throughput. The network focused on QoS being affected by a wormhole attack and established foundation for future work toward designing a mechanism to identify nodes and links actively involved in wormhole attacks.

Woungang et al., [3] proposed a modified AODV to detect and reaction of Wormhole Attack named as AODV-WADR-AES. This protocol used Advanced Encryption Standard (AES) for secure routing against wormhole attacks. The method in the paper has replaced by another security algorithm triple DES algorithm, and this aimed to reduce the end-to-end delay and packet delivery ratio of the wormhole traversed link.

Chaurasia et al., [4] an efficient wormhole attack detection method named Modified wormhole detection AODV protocol (MAODV) protocol was proposed. Number of hops from source to destination and delay of a node in varied paths was used for detection of Wormhole attack detection. Simulations justified the performance of MAODV protocol and the destination was able to detect wormhole attacks.

Singh et al., [5] proposed a wormhole resistant hybrid technique named as WRHT to detect the presence of wormhole attack. The technique follows the watchdog mechanism and Delphi schemes. The technique also provided the probability of the wormhole attack presence and ranks according to that. This doesn't belong with additional hardware and the cryptographic schemes. So the computation cost is reduced in the WRHT.

Kaur et al., [6] proposed a novel wormhole attack detection technique to identify the wormhole link by utilizing the end-to end delay.

This communication delay analysis technique acquires the exact delay for the normal link and wormhole links. As like the WHT, it does not require the GPS, clock synchronization and special hardware to detect the wormhole attack. The technique calculates the threshold values to identify the wormhole link,

however the threshold calculation may affect by traffic in the heterogeneous networks.

S.NO	TITLE	AUTHORS	TECHNIQUES	ADVANTAGES	DISADVANTAGES
1	Packet leashes: a defense against wormhole attacks in wireless networks	YC Hu, A Perrig, DB Johnson	TIK protocol and Merkle hash tree	Protects against replay, spoofing, and wormhole attacks, and ensures strongly that there is no modification in the data	Less efficient require broadcast authentication, precise time synchronization is not easily achievable.
2	A study on wormhole attacks in MANET	Maulik, Reshmi, and Nabendu Chaki.	The Reference Point Group Mobility Model (RPGM)	The authors considered multiple QOS parameters	Traffic attracted by the false link advertised by the colluding nodes
3	Comparison of two security protocols for preventing packet dropping and message tampering attacks on AODV-based mobile ad Hoc networks.	Woungang, Isaac, Sanjay Kumar Dhurandher, Vincent Koo, and Issa Traore.	AODV-WADR-AES	Helps to detect the existence of wormhole attack in the network	mobile devices that are incompatible with AES
4	MAODV: Modified wormhole detection AODV protocol.	Chaurasia, Umesh Kumar, and Varsha Singh.	MAODV	It does not require any special hardware such as directional antenna and it does not require clock synchronization and positioning system. detects the legitimate path and wormhole path in the network efficiently	The MAODV does not work well when all the paths are wormhole affected.
5	.WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks	Singh, Rupinder, Jatinder Singh, and Ravinder Singh	WRHT (watchdog and Delphi)	Hidden mode allows fast detection.	Suitable for only sensor networks
6	Wormhole Attack Detection Technique in Mobile Ad Hoc Networks	Kaur, Parvinder, Dalveer Kaur, and Rajiv Mahajan	Threshold calculation technique	Doesn’t require special hardware and reduces the cost	Not suitable for the heterogeneous networks

Table 1. Summary of Wormhole detection technique

Summary:

All of the above solutions are implemented by protocol modification, by using special hardware, some avoids hardware usage or by using extra nodes to monitor the network traffic. Each method has its own strengths and weaknesses. The protocol modification may have extra overhead or cause delay in the route discovery process. The use of special hardware can be expensive or resource starving. And many techniques utilized the end-to-end delay calculation to detect the wormhole link, but it is not an appropriate feature for the wormhole detection. The use of extra nodes can increase the deployment cost but does not have the threat of wormhole declaration by a single (normal or malicious) node. The overall drawback of the above mentioned techniques shown in table 1.Based on statistical analysis and observation without special nodes, any additional hardware the wormhole prevention and detection should be made.

Sinkhole attack detection and prevention techniques:

In MANET security, many attacks are studied. One of the important and undetectable attacks is sinkhole attack. This will arise in the network layer. In this kind of attack all the mobile nodes are attracted by the vulnerable sinkhole node, which makes the fake routing and resource information’s for the other nodes to acquire their data.

Marti et al., [7] attempted to mitigate routing misbehaviors and sinkhole nodes in MANET using Watchdog techniques. The authors used DSR protocol to develop the scheme. To identify the malicious behavior of a node, the node sending the traffic observes promiscuously the transmission of the neighboring node and route. If the neighbor node interrupts the data transmission, then the node will be considered as a misbehaving node. The misbehaving node will not be allowed in the further transaction. The watchdog maintains a copy of recently sent packets and compares each overheard packet with the packets it holds in order to find the similarity. If they are similar, the packet in the buffer is deleted. If a certain packet is in the buffer beyond certain time, the watchdog increments a failure tally for the node which should have forwarded the packet by one. Once, that counter exceeds a certain threshold value, it concludes that the node is malicious and sends a notification to the source node. The trust calculation in this method is based on the watchdog mechanism.

Kim et al., [8] proposed a cooperative sinkhole detection method. This analyzes the sinkhole attack and extracts the features for the sinkhole attack. The sinkhole detection algorithm developed with the reduction of time and cost. When a mobile node is in the reception of route request message having the originator ID equal to that of receiving mobile node, it examines sequence number of message. If the sequence number in the route request message is higher to the present sequence number of the mobile node, the current node identifies the presence of sinkhole node; also it concludes that the RREQ message comes from sinkhole node. Hence, it is concluded that the route path of the request message contains sinkhole node. However, in practical scenario, not all the fake route request messages reach the victim node and the sinkhole node will not be detected.

Vishnu et al., [9] studied the usage of backbone network and assigns constrained IP addresses to the afresh mobile nodes. Authors proposed a complete protocol for detection & removal of networking Black/Gray Hole When a node wants to send the data traffic to the destination node, it checks for an unused IP. The route request message is broadcasted for the destination and the RIP addresses. This IP address is unknown to the nodes which are other than the nodes in backbone network. If the originating node receives a route reply packet having the route for this constrained IP address, it denotes the presence of sinkhole node en route. This method requires a trusted third party, which is very difficult to achieve in MANET environment. Further this method requires all the nodes to be in the promiscuous mode to monitor the activities of the suspected node.

Stafrace et al., [10] designed an agent based framework modeled over a military command structure and an agent behavioral model. This model uses adapted military tactics to police routes, and detect intruders in the network. The agents follow a risk-based approach such that the frequency of patrols is directly proportional to the risk factor of the route. In this study, a simulation-based model detects and recover from a Sinkhole attack in a Wireless Sensor Network, using the AODV is implemented.

Gagandeep. G et al., [11] authors focused on sinkhole attacks on routing protocols such as DSR, AODV and proposed a Security-aware routing (SAR) technique to reduce the impact of sinkhole attack. SAR performs the routing message protection and Routing update protection processes.

Shafiei et al., [12] presented a distributed detection technique for sinkhole attack. Few of the nodes in the MANET are considered as trusted nodes. These trusted nodes act as monitoring nodes. Each of the monitoring nodes contains the local information about the network. Furthermore, the detection operation requires a base station.

These assumptions and requirements are not suitable for the MANET environment. Moreover, the trusted node can be compromised.

S.NO	TITLE	AUTHORS	TECHNIQUES	ADVANTAGES	DISADVANTAGES
7	Mitigating routing misbehavior in mobile ad hoc networks	Marti, Sergio, Thomas J. Giuli, Kevin Lai, and Mary Baker	DSR protocol and watchdog	Techniques increase throughput by 17%	Excessive overhead. Failed to detect malicious nodes in the high mobility nodes
8	A cooperative-sinkhole detection method for mobile ad hoc networks	Kim, Gisung, Younggoo Han, and Sehun Kim.	Cooperative sink hole detection technique	Reduces detection time Less sensitive to topology change	Increased network overhead
9	Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks	Vishnu, K., and Amos J. Paul	Packet information based techniques	Detects the presence of sinkhole node en route	This method requires a trusted third party.
10	Military tactics in agent-based sinkhole attack detection for wireless ad hoc networks	Stafrace, Stefan K., and Nick Antonopoulos	AODV and agent behavioral mode	Reduces detection time Less sensitive to topology change	Increased network overhead
11	Study on sinkhole attacks in wireless Ad hoc networks	Gagandeep. G and Aashima. A	DSR, AODV SAR (security aware routing)	Security Capabilities it deals with ability to handle various security features. Trust hierarchy SAR supports hierarchy of trust levels among various available routes.	Authentication process need much time.
12	Detection and mitigation of sinkhole attacks in wireless sensor networks	Shafiei, Hosein, Ahmad Khonsari, H. Derakhshi and P. Mousavi	Distributed detection technique	Trusted nodes act as monitoring nodes. Each of the monitoring nodes contains the local information about the network.	Assumptions and requirements are not suitable for the MANET environment. Moreover, the trusted node can be compromised.

Table 2. Summary of sinkhole detection technique

Summary:

All of the above techniques provides a comprehensive literature review of the existing methodologies to mitigate sinkhole attacks in MANET. The intrusion detection systems, cluster based intrusion detection and cryptographic based detection systems either require centralized authority in the MANET or poses higher computational and routing overhead. The overall comparison of the existing sinkhole detection techniques are given in table 2. These decline the performance of the mobile ad hoc network in terms of routing overhead, packet delivery ratio and end-to-end delay. Hence, efficient methodology to detect and isolate sinkhole nodes in MANET is required.

III. CONCLUSION

In this paper, a summarization of wormhole and sinkhole attacks in MANET is investigated. MANET security is the most predominant area of research. This paper summarized various wormhole and sinkhole prevention and detection schemes. Most of the techniques are based on the hop sequence verification, trust based and neighbor analysis approaches. Finally, it is concluded that the existing schemes for preventing the wormhole and sinkhole attacks using the routing protocols AODV and DSR are need additional concentration on detection such attacks. So there is no adequate technique or protocol available for detecting multiple attacks. So it is required to design a secure routing protocol with energy efficient attack handling system to prevent the security threats.

REFERENCES

[1] YC Hu, A Perrig, DB Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks." *In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, vol. 3*, pp. 1976-1986. IEEE, 2003.

[2] Maulik, Reshmi, and Nabendu Chaki, "A study on wormhole attacks in MANET*." International Journal of Computer Information Systems and Industrial Management Applications 3, no. 1*, pp. 271-279, 2011.

[3] Woungang, Isaac, Sanjay Kumar Dhurandher, Vincent Koo, and Issa Traore, "Comparison of two security protocols for preventing packet dropping and message tampering attacks on AODV-based mobile ad Hoc networks." *In Globecom Workshops (GC Wkshps), 2012 IEEE*, pp. 1037-1041, IEEE 2012.

[4] Chaurasia, Umesh Kumar, and Varsha Singh, "MAODV: Modified wormhole detection AODV protocol." *Sixth International Conference on Contemporary Computing (IC3) IEEE*, pp. 239-243, 2013.

[5] Singh, Rupinder, Jatinder Singh, and Ravinder Singh, "WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks." *Mobile Information Systems* (2016).

[6] Kaur, Parvinder, Dalveer Kaur, and Rajiv Mahajan. "Wormhole Attack Detection Technique in Mobile Ad Hoc Networks." *Wireless Personal Communications*, pp.1-12, 2011

[7] Marti, Sergio, Thomas J. Giuli, Kevin Lai and Mary Baker. "Mitigating routing misbehavior in mobile ad hoc networks." *In Proceedings of the 6th annual international conference on Mobile computing and networking*, pp. 255-265, ACM 2000.

[8] Kim, Gisung, Younggoo Han and Sehun Kim. "A cooperative-sinkhole detection method for mobile ad hoc networks." *AEU-International Journal of Electronics and Communications 64, no. 5*, pp. 390-397, 2010.

[9] Vishnu, K., and Amos J. Paul. "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks." *International Journal of Computer Applications 1, no. 22* (2010): 38-42.

[10] Stafrace, Stefan K. and Nick Antonopoulos. "Military tactics in agent-based sinkhole attack detection for wireless ad hoc networks." *Computer Communications 33, no. 5* (2010): 619-638.

[11] Gagandeep, G and Aashima, A. "Study on sinkhole attacks in wireless Ad hoc networks*". International journal on computer science and engineering* (2012): 4-6.

[12] Shafiei, Hosein, Ahmad Khonsari, H. Derakhshi, and P. Mousavi. "Detection and mitigation of sinkhole attacks in wireless sensor networks*." Journal of Computer and System Sciences 80, no. 3* (2014): 644-653.

[13] Gandhewar, Nisarg, and Rahila Patel. "Detection and Prevention of sinkhole attack on AODV Protocol in Mobile Adhoc Network." *Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on. IEEE 2012.*

International Journal of Engineering Research and Applications (IJERA) is **UGC approved** Journal with Sl. No. 4525, Journal no. 47088. Indexed in Cross Ref, Index Copernicus (ICV 80.82), NASA, Ads, Researcher Id Thomson Reuters, DOAJ.

D.Sasirekha A Survey on Wormhole and Sinkhole Attack Detection and Prevention Techniques in Manet." International Journal of Engineering Research and Applications (IJERA) , vol. 7, no. 11, 2017, pp. 80-85.