International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

Investigation of Detection & Prevention Sinkhole attack in MANET

Ashok Kumar Mishra[1], Prof. Gajendra Singh[2], Prof. Kailash Patidar[3]
Department of Computer Science and Engineering
SSSIST, Sehore, India
[1]ashokmishra1987@gmail.com, [2]gajendrasingh86@rediffmail.com, [3]kailashpatidar123@gmail.com

Abstract:- The sensor nodes in the network are forming independent network. The limited range sensors maintain the link up to destination in Mobile Ad hoc Network (MANET). In this network nodes are communicate in open medium and by that the communication among the mobile nodes are perform without any centralized authority that's why network security is one of the most important issue in MANET. There are many attackers in MANET like sinkhole attack drop the data packets in network with the support of neighbour attacker. To overcome the disputes, there is a need to build a prevailing security solution i.e. IDS (Intrusion Detection System) that achieves both extensive protection and desirable network performance. The proposed work analyze the profile of each node in network by that malicious effect information is retrieve and IDS is block the malicious activities of attacker. This work analyzes the effect of sinkhole attack through malicious nodes which is probable attacks in MANET The data packets do not reach the destination by that due to this attack, data loss will occur. The damage will be serious if malicious node in a network working as an attacker node absorbs all data packets delivered through them. In this research we proposed a simple IDS Algorithm against dropping attack and measure the network performance after applying IDS. We simulated dropping attacks in network simulator 2 (ns-2) and measured the packet loss in the presence of attacker and in presence of Intrusion Detection System against malicious attack. Our solution improved the 90% network performance in the presence of a packer dropping attacker.

Keywords: - Sinkhole attack, IDS, Routing, AODV, Security.

I. INTRODUCTION

Wireless sensing element networks (WSNs) have full-grown in importance as an affordable resolution for knowledge activity and assortment. A key advantage of WSNs is their easy preparation, partially owing to their use of routing protocols that self-configure the network [1, 2]. However, if WSNs area unit to be accustomed monitor important infrastructure, like water distribution, then it's essential that the integrity of the WSN be protected against malicious attacks. Especially, the routing protocols used with WSNs area unit doubtless susceptible to routing attacks, which may disrupt property within the network. While traditional cryptographic defences are used to protect wired networks, the limited communication and Central processing unit resources in low-cost wireless sensor nodes makes resource intensive cryptography impractical. Sinkhole attacks (see Figure 1 generally work by creating a compromised node look particularly engaging to close nodes with reference to the routing formula. For example, a person might spoof or replay an advert for a particularly top quality route to a bachelor's degree. Some protocols may truly try and verify the standard of route with end-to-end acknowledgements containing responsibility or latency info.

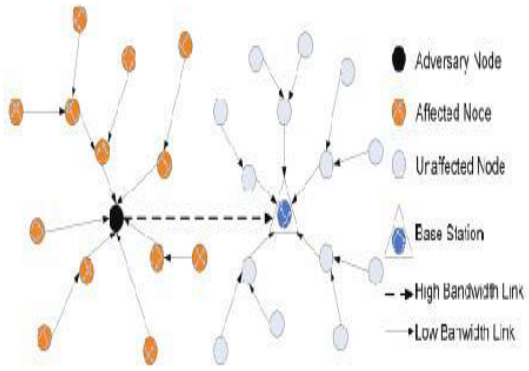

Figure 1: Sinkhole Attack

During this case, a laptop-class person with a robust transmitter will truly offer a top quality route by sending with enough power to achieve the bachelor's degree in a very single hop, or by employing a hollow attack. Due to either the important or fanciful top quality route through the compromised node, it's doubtless every neighboring node of the person can forward packets destined for a bachelor's degree through the person, and additionally propagate the attractiveness of the route to its neighbors. Effectively, the adversary creates a large "sphere of influence", attracting all traffics destined for a BS from nodes several hops away from the compromised node. The bottom station is prevented by the depression attack from achieving complete and correct sensing knowledge, and so it's resulted in a crucial threat that is important for wireless sensing element networks. In fact, this happens owing to the unprotected wireless links, the preparation of the sensors in open areas, and also the weak computation and battery power. The present routing protocols in sensing element networks show typically vulnerability to the depression attack [1]. Some studies have suggested several secure mechanisms to use as cryptographic methods for protecting network however, they are mostly localized, or there is a high computation and also a requirement for time synchronization among the nodes. We present a new lightweight algorithm in order to detect the sinkhole attack and to recognize the engaged intruder [3, 4]. Two main elements may be explained for this technique; a secure and low-overhead formula and an economical identification formula. The primary one could be a protected and low overhead formula for the bottom station which may collect the network flow info from the attacked space. The other is a formula able to analyze the routing pattern and establish the trespasser.

II. RELATED WORK

Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala [1] "Detection of Sinkhole Attack in Wireless Sensor Networks" this title suggests an algorithm which firstly finds a group of suspected nodes by analyzing the consistency of data. Then, the intruder is recognized efficiently in the group by checking the network flow information. The proposed algorithm's performance has been evaluated by using numerical analysis and simulations. Therefore, accuracy and efficiency of algorithm would be verified. Rajakumaran, Thamarai Selvi, [5] "Detection Techniques of Sinkhole Attack in WSNs: A Survey" This title discus about various detection techniques for the sinkhole attacks in WSN. Vinay Soni, Pratik Modi, Vishvash Chaudhri [6]"Detecting Sinkhole Attack in Wireless Sensor" in this title we discuss there are many possible attacks on sensor network such as selective forwarding, jamming, sinkhole, wormhole, Sybil and hello flood attacks. Sinkhole attack is among the most destructive routing attacks for these networks. It may cause the intruder to lure all or most of the data flow that has to be captured at the base station. Once sinkhole attack has been implemented and the adversary node has started to work as network member in the data routing, it can apply some more threats such as black hole or gray hole. Ultimately this drop of some important data packets can disrupt the sensor networks completely. Md. Ibrahim Abdullah, Mohammad Muntasir Rahman and Mukul Chandra Roy, [7] "Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count" In this title, a mechanism is proposed against sinkhole attacks which detect malicious nodes using hop counting. The main advantage of the proposed technique is that, a node can detects malicious nodes only collaborating with the neighbor nodes without requiring any negotiation with the base station. Simulation result shows that, the proposed technique successfully detects the sinkhole nodes for large sensor field. Gagandeep, Aashima, [8] "Study on Sinkhole Attacks in Wireless Ad hoc Networks" This paper focuses on sinkhole attacks on routing protocols such as DSR, AODV. To overcome the problems occur due to sinkhole we discuss about Security-aware routing (SAR) which helps to reduce the impact of such attack. Kesav Unnithan S , Lakshmi Devi , Sreekuttan Unnithan,[9] "Survey of Detection of Sinkhole Attack in Wireless Sensor Network" This title focuses on the various methods that can be implemented to overcome this attack like Location Based Compromise Tolerant Security Mechanism, Hop Count Monitoring Scheme and through Non Cryptographic Method of Sinkhole Attack Detection. Sonal R. Jathe, Dhananjay M. Dakhane, [10] "Indicators for Detecting Sinkhole Attack in MANET" Our title particularly studies sinkhole attack and different parameters of sinkhole detection. Kripasinh Gohil [11] "Detection of Sinkhole attack in Wireless Sensor Networks using Mobile agent and multiple Base stations" in this we discuss technique is to detect the sinkhole attack using multiple base stations and a mobile agent based technology. Multiple base stations ensure high packet delivery rate. Mobile agent is a software program which is self controlling and it moves from node to node and checks the presence of sinkhole nodes in the network. Vivek Tank, Amit Lathigara, [12]"To Detect and Overcome Sinkhole Attack in Mobile Ad hoc Network" in this title we are discuss to Due to the property of self-deliberate, where all point of network behaves like source or router and also all nodes are keeps on moving freely in network area. Mobile ad hoc network perform important role in connectionless environment. Security is the most fundamental requirement in mobile ad hoc network to secure the sensitive information from hackers. In MANETs typically many attacks are routing protocol attacks. Sinkhole attack is one of the most severe attacks in MANETs. It tries to attract all neighbor nodes to itself and broadcast fake or bogus routing path. Here sinkhole attack describes in AODV routing protocol to applying security by using digital signature and hash chain to prevent the attack. Amrit Pal Singh, Parminder Singh, Rakesh Kumar [13] "A Review on Impact of Sinkhole Attack in Wireless Sensor Networks" In this title we are using clustering technique along with replicated mobile agents to prevent the wireless sensor network from sinkhole attacks. We use mobile agents to aware every node from its trusted neighbors so they do not listen to the traffics generated by malicious nodes. We evaluate our work in terms of packet loss rate, throughput and end to end delay.

III. OBJECTIVE

Mobile ad-hoc network security is critical challenge because its nature is independent network creation with frequently topology changes. That's why MANET is survival from physical to application layer unsecure. But security is measure issue for the communication so we study number of prevention mechanism and protect the ad-hoc network through different attack. In this thesis our basic objective to protect the ad-hoc network through sinkhole attacks. Sinkhole attack is a type of attack were compromised node tries to attract network traffic by advertise 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.

IV. PROBLEM STATEMENT

Mobile ad hoc communication security is very challenging issue because lack of trusted infrastructure as well as dynamic network behaviour. Mobile ad hoc network not guaranteed the quality of service for reliable data delivery to the receivers. So in this dissertation our motive to design a collaborative trusts mechanism against sinkhole attack and to provide secures communication to the receivers.

V. PROPOSED WORK

Mobile ad hoc network is a temporary autonomous system, where every communication take place faith bases, but cannot guaranteed that our data will successful delivery to the legitimate user. Before that proposal we study number of paper against quality of service, trust mechanism, reliability and security against sink hole attack, but they not cover all aspect of network parameter and also identifies that some improvement are needed on the existing work. So in the proposed approach we design the distributed trust methodology and achieve the QoS requirement for reliable service. In distributed trust mechanism every node watch the activity of neighbor nodes and calculate the trust level, based on receives and

forwarding data criteria, the trust level is ranging between 0 to 1, that trust factor every neighbor nodes are calculated by timely manner, And combine the trust level of particular node (suspicious) in the single area (whose reliability or trust level all the node set initially 1), that node calculate average trust value of particular node (suspicious) and while trust values lower than the fifty percentage so further that is under second time (suspicious) re-watch the node and similar property exist than block that particular node else trust level increases. That work collaborative calculates the node trust and time to time increase trust level of the node and helps to identify attacker node. In our approach trust level calculate against the sink hole attack, cannot decrease the trust level while data are drop by network depended reason i.e. congestion, collision, MAC error etc. for network error minimization be appropriate routing are modified that aware the channel is an ideal or engaged and also collision are resolve so our QoS maintain. Proposed approach provides the reliable path from sender to receiver with all aspect of QoS requirements. That increases the packet delivery ratio and decreases the overhead of the network.

VI. SIMULATION ENVIRONMENT

Simulation will be done in Network Simulator- 2 (NS-2). The description about simulation environment is as follows: Network simulator 2 (NS2) is the result of an on-going effort of research and development that is administrated by researchers at Berkeley [14]. It is a discrete event simulator targeted at networking research. It provides substantial support for simulation of TCP, routing, and multipath protocol. The simulator is written in C++ and a script language called OTcl2. Ns use an Otcl interpreter towards the user. This means that the user writes an OTcl script that defines the network (number of nodes, links), the traffic in the network (sources, destinations, type of traffic) and which protocols it will use. This script is then used by ns during the simulations.

VII. CONCLUSION

The Mobile Ad hoc Network (MANET) is a dynamic cost-effective network and provides communication with random movement of mobile nodes. The security is the major problem in this kind of decentralized network. The centralized administrator control absence is venerable to network from different attacks. In this research we study the sinkhole attack, security and normal routing in networks and find its affects. In our study, we used the AODV routing protocol. But the other various routing protocols could be simulated also in previously. The proposed scheme resolves cooperative effect of sinkhole attack in the network. But the detection of the sinkhole attack is possible through proposed IDS security scheme.

REFERENCES

[1]. Ahmad Salehi S., M.A. Razzaque, Parisa Naraei, Ali Farrokhtala "Detection of Sinkhole Attack in Wireless Sensor Networks" Proceeding of the 2013 IEEE International Conference on Space Science and Communication (IconSpace), 1-3 July 2013, Melaka, Malaysia.

[2]. Ngai, E. C. H., Liu, J. and Lyu, M. R. An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. Computer communication, 2007. Elsevier locate. 2353-2364

[3]. Choi, B. G., Cho, H. E., Hong, C. S. and Kim, J. H. A sinkhole Attack detection Mechanism for LQI based Mesh Routing in Wireless Sensor Networks. International conference wireless security. 21-24 January (2008). Korea. 65-8

[4]. Razzaque, M., et al. Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead. Wireless Networks and Security, Springer 2013.

[5]. Rajakumaran, Thamarai Selvi, "Detection Techniques of Sinkhole Attack in WSNs: A Survey" International Journal of Engineering Science Invention Volume 3 Issue 6‖ June 2014 ‖ PP.12-14.

[6]. Vinay Soni, Pratik Modi, Vishvash Chaudhri "Detecting Sinkhole Attack in Wireless Sensor Network" (IJAIEM) Vol. 2, Issue 2, February 2013.

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

[8]. GAGANDEEP, AASHIMA, "Study on Sinkhole Attacks in Wireless Ad hoc Networks" Gagandeep et al. / International Journal on Computer Science and Engineering (IJCSE) Vol. 4 No. 06 June 2012.

[9]. Kesav Unnithan S , Lakshmi Devi , Sreekuttan Unnithan, "Survey of Detection of Sinkhole Attack in Wireless Sensor Network" Kesav Unnithan S L et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (6) , 2015, 4904-4909.

[10]. Sonal R. Jathe, Dhananjay M. Dakhane, "Indicators for Detecting Sinkhole Attack in MANET" International Journal of Emerging Technology and Advanced Engineering Vol. 2, Iss. 1, January 2012.

[11]. Kripasinh Gohil "Detection of Sinkhole attack in Wireless Sensor Networks using Mobile agent and multiple Base stations" volume Issue 5 may 2014 IJOURNALS.

[12]. Vivek Tank, Amit Lathigara, "To Detect and Overcome Sinkhole Attack in Mobile Ad hoc Network" Volume 2 – No.6, August 2015.

[13]. Amrit Pal Singh, Parminder Singh, Rakesh Kumar "A Review on Impact of Sinkhole Attack in Wireless Sensor Networks" IJARCSSE Volume 5, Issue 8, August 2015.

[14]. http://www.isi.edu/nsnam/ns/