Gray-Hole Attack Minimization based on contradiction for ad-hoc networks

Suha Farheen taj H N[1], Chinnaswamy C N[2], Sunil Kumar B V[3], Varshika S[4], & Supriya S[5]

[1,3,4,5] B.E Dept of ISE, NIE, Mysuru, Karnataka, India
[2]Assocaiate Professor Dept of ISE, NIE, Mysuru, Karnataka, India.

---***---

***Abstract** - The development for other rising advance technology for example, IoT and portable information correspondence frameworks are sought after for security purposes. A strategy for limiting the Gray-Hole attack in an AD-HOC arrange is necessary for better information recovery. This attack don't work after the attack has initiated, it utilizes the interior learning of the AODV protocol and OLSR protocol to avoid the Gray-Hole attack. Mobile ad-hoc network (MANET) is a remote arrange that can exchange the data from source to goal remotely, Because of the open open communication media the portable specially appointed organize has some security limitations there are the possibility of information leakage in the network Gray-hole attack, black-hole attack, wormhole attack are the major threats in the mobile ad-hoc network. In Gray-hole attack specific dropping of the bundles happens, and the data can't be additionally transmitted .this paper examine the proper arrangements and built up the reasonable arrangement to keep the system from the Gray- hole attack.*

***Key Words**: MANET, Gray-hole attack, DCFM, OLSR, AODV.*

1. INTRODUCTION

A mobile ad hoc network *(MANET)* is generally defined as a network that has many free or autonomous nodes, often composed of mobile devices or other mobile pieces, that can arrange themselves in various ways and operate without strict top-down network administration.[4] There are many different types of setups that could be called MANETs Some use 4G networks and other systems as examples of a potential topology for a MANET, while others refer to a vehicular ad-hoc network, where the free network nodes are installed in cars and other vehicles.

The security threats have been extensively discussed and investigated in the wired and wireless networks, the correspondingly perplexing situation has also happened in MANET due to the inherent design defects. There are many security issues which have been studied in recent years. For instance, snooping attacks, wormhole attacks, black hole attacks, routing table overflow and poisoning attacks, packet replication, denial of service (DoS) attacks, distributed DoS (DDoS) attacks, et cetera Especially, the misbehavior routing problem is one of the popularized security threats such as black hole attacks. Some researchers propose their secure routing idea to solve this issue, but the security problem is still unable to prevent completely. blackhole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes. One cause mentioned in research is through a denial-of-service attack on the router using a known DDoS tool. Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent.

The malicious router can also accomplish this attack selectively, e.g. by dropping packets for a particular network destination, at a certain time of the day, a packet every *n* packets or every second, or a randomly selected portion of the packets.

This is rather called a grey hole attack. rendering anti-blackhole algorithms is useless . Thus, mitigation of the gray-hole attack will also solve the more famous black-hole attack as well.

Optimized Link State Routing (OLSR) protocol is a MANET routing protocol and is evaluated mainly for two things. Primarily OLSR is less secure like AODV and others. The reason for it being less secure is that it is a table-driven in nature and uses a methodology called selective flooding technique, where redundancy is reduced and thus the security possibilities of the protocol is reduced. Another reason for selecting OLSR is that is an highly effective routing protocol for MANET. A brief information about formal routing is provided by the proposed methodology termed Denial Contradictions with Fictitious Node Mechanism (DCFM) which provides brief information about formal routing. Here, fictitious node acts as a virtual node and large networks are managed from attacks

2.Related work

1.In recent papers, [1] Nadav Schweitzer, Ariel Stulman, Member, IEEE, Asaf Shabtai and Roy David Marg alit proposed a method for Gary- Hole attack detection. In any case, it doesn't fulfil every one of the information that must be sent. It has the burdens, for example, doesn't illuminate the source about the information failure. It can't recognize the redress goal hub, Time utilization is high, Packet's proficiency is low.

2.Sukla Banerjee proposed a mechanism for detection/removal of cooperative black and GrayHole attack in mobile ad-hoc networks. In this instead of sending the total data traffic at a tie it divides the total traffic into some small sized blocks. So that malicious nodes can be detected and removed in between the transmission of two such blocks by ensuring an end-to-end checking. Source node sends a prelude message to the destination node before start of the sending any block to alert it about the incoming data block. It is time consuming algorithm it takes time in converting of total traffic into small sized blocks

3. Toutouh [1] Recent advances in wireless technologies have given rise to the emergence of vehicular ad hoc networks (VANETs). In such networks, the limited coverage of WiFi and the high mobility of the nodes generate frequent topology changes and network fragmentations. For these reasons, and taking into account that there is no central manager entity, routing packets through the network is a challenging task. Therefore, offering an efficient routing strategy is crucial to the deployment of VANETs. This paper deals with the optimal parameter setting of the optimized link state routing (OLSR), which is a well-known mobile ad hoc network routing protocol, by defining an optimization problem. This way, a series of representative metaheuristic algorithms (particle swarm optimization, differential evolution, genetic algorithm, and simulated annealing) are studied in this paper to find automatically optimal configurations of this routing protocol. In addition, a set of realistic VANET scenarios (based in the city of Malaga) have been defined to accurately evaluate the performance of the network under our automatic OLSR. In the experiments, our tuned OLSR configurations result in better quality of service (QoS) than the standard request for comments (RFC), as well as several human experts, making it amenable for utilization in VANET configurations.

4. Y.-C. Hu, [3] As mobile ad hoc network applications are deployed, security emerges as a central requirement. In this paper, we introduce the wormhole attack, a severe attack in ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts, and even if all communication provides authenticity and confidentiality.

In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. For example, most existing ad hoc network routing protocols, without some mechanism to defend against the wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication. We present a general mechanism, called packet leashes, for detecting and, thus defending against wormhole attacks, and we present a specific protocol, called TIK, that implements leashes. We also discuss topology-based wormhole detection, and show that it is impossible for these approaches to detect some wormhole topologies.

3.Existing System

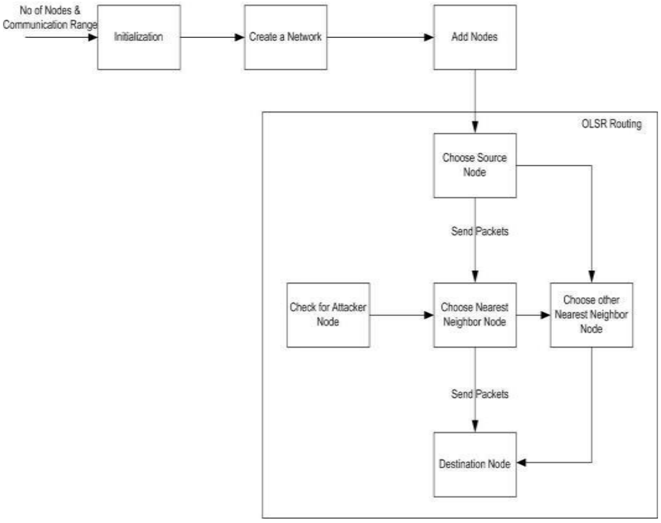
Mobile ad-hoc network (MANET) is decentralized system, in this system hubs can move progressively. OSI Network layer faces a few attack. Gray hole attack chip away at most notable succession number amid Replay message, a gathering of gray hole hubs effectively utilized against steering in MANET called community gray hole attack

4.Proposed system

An OLSR based system is helpless against gray hole attack. The aggressor may send, for example, a sham HELLO messages to its one-jump neighbors, asserting to know more one-bounce neighbors than it really does. This will misguidedly build its likelihood of being picked as a sole MPR by its neighbors. The more neighbors an aggressor cases to have, the bigger the potential effect of the attack.

Denial Contradictions with Fictitious Mechanism Node Component DCFM was proposed by so as to address the problem of hub privacy in OLSR based systems. It recognizes potential malicious hubs attempting to adulterate HELLO messages utilizing just interior data inside the casualty, without depending on any brought together or outer confided in party. Such early discovery keeps a conceivable attack before it can manifest. DCFM confirms the legitimacy of a HELLO message by searching for logical inconsistencies between what the message claims also, its pre-gained topological information. As indicated by ,DCFM, sole MPRs assignments are permitted just when no logical inconsistencies are found. With the nearness of contradictions, a MPR can be assigned for every one of the two-bounce neighbors for which the presumed hub is the main access point. It cannot, be that as it may, be assigned as sole MPR for two jump neighbors that can be come to through different ways. Following , and as defended in , in this work we accept that TC messages can't be restock.

5. System Architecture



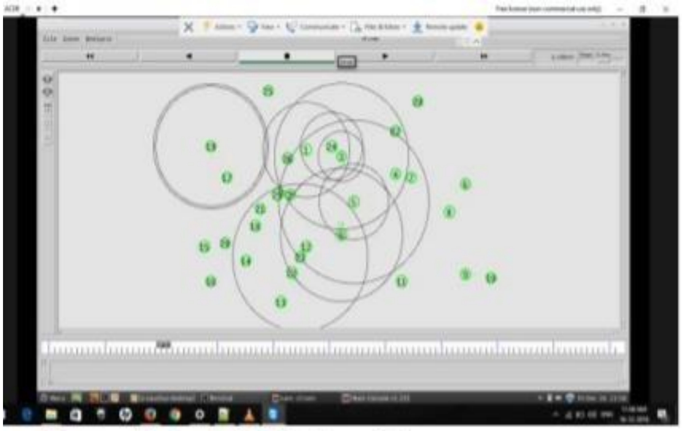
In the above diagram, number of nodes and communication range has been initialized and configured into network simulator, and then select the routing path in the network. In the selected path send the data from source node to destination node through the neighbour node using nearest next hop approach. If any DOS attack detected in the path, find the attacked neighbour nodes and mark it as attacker node. Finally data should send from source node to destination node through non attacker neighbour nodes by applying OLSR Routing approach.

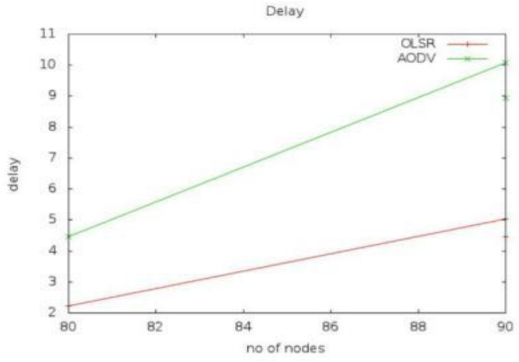
6.Performance Analysis

6.1 Simulation

Simulation is the imitation of the operation of a real-world process or system.[1] The act of simulating something first requires that a model be developed; this model represents the key characteristics, behaviours and functions of the selected physical or abstract system or process. The model represents the system itself, whereas the simulation represents the operation of the system over time.. Using mathematical formulas, or actually capturing and playing back observations from a production network. The behaviour of the network and the various applications and services it supports can then be observed in a test lab; various attributes of the environment can also be modified in a controlled manner to assess how the network would behave under different conditions.

6.2Experimental result





7.Conclusion

This paper introduces a change calculation for OLSR based systems for moderating Gray-hole attack . Utilizing exclusively inward learning picked up by taking an interest hubs, we can decline caught parcels by a two fold digit factor; well past what DCFM alone can achieve under comparable conditions. Single supposition is a dynamic attacker attempt to malicious impact arrange topology to build the attack surface. dormant attackers who can at present go undetected can likewise drop bundles, they can't ensure that courses will go through them fundamentally supporting the likelihood of attack achievement.

8. REFERENCES

[1] J. Toutouh, J. Garcia-Nieto, and E. Alba, “Intelligent OLSR routing protocol optimization for VANETs,” IEEE Trans. Veh. Technol., vol. 61, no. 4, pp. 1884– 1894, May 2012.

[2]. "Contradiction Based Gray-Hole Attack in Ad-Hoc Networks" Nadav Schweitzer, Ariel Stulman, Member, Asaf Shabtai and Roy David Margalit IEEE Transactions on Vehicular Technology, vol. 61, no. 4, pp. 1884–1894, May 2012

[3]. Y.-C. Hu, A. Perrig, and D. B. Johnson, “Wormhole attacks in wireless networks,” IEEE Journal on Selected Areas in Communications, vol. 24,no. 2, pp. 370–380, Feb 2006

[4]https://www.techopedia.com/definition/5532/mobile-adhoc-network-manet

[5]https://en.wikipedia.org/wiki/Packet_drop_attack
[6]. H. Deng, H. Li, and D.P. Agrawal, “Routing security in wireless a hoc networks,” IEEE Communications Magazine, October 2002.