Journal of Theoretical and Applied Information Technology
10th February 2016. Vol.84. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A PROPOSAL FOR MITIGATION OF GRAY HOLE ATTACK IN WIRELESS MESH AD-HOC NETWORKS USING S-DSDV

K.SUMANTH[1] DR.SRIDEVI GUTTA[2] DR. SYED UMAR[3] DR.K.KIRAN KUMAR[4] DR. MD ALI HUSSAIN[5]

[1]M.Tech. Student, Dept. of CSE, K L University, Guntur Dist.
[2] Professor, Dept. of CSE, K L University, Guntur Dist.
[3]Assoc. Professor, Dept. of CSE, K L University, Guntur Dist.

[4]Professor, Dept. of ECM, K L University, Guntur Dist.

[5]Professor, Dept. of ECM, K L University, Guntur Dist.

ABSTRACT

Wireless Mesh Networks have its desired features like Self-organization and self-configuration it provides advantages for Wireless Mesh Networks like market coverage, scalability, good reliability and low upfront cost. These networks have an effective quality that they are ease of scalability with heterogeneous multi-hop with very low cost. It is a mobile which is of connectionless-oriented and vigorous traffic of the routed packets. These infrastructure network forms the multi-^{hop} transmission of data packets from peripherals and forms the multiple chains of WLANS. In Wireless Mesh Networks, security is a limitation and which can be overhead easily. Small analysis of this had explained in this paper like security threats such as GRAY HOLE ATTACK [GHA] in DSDV routing protocol. GHA is a special type of DOS attack which is similar to black hole attack which will change the state to various states like selective packet dropping is challenging one. With the effect of this GHA there will be impact on various parameters like E2E delay, throughput etc., A variety of Gray Hole attack solutions have been proposed in the literature. We surveyed and identified different detection and mitigation techniques of Gray Hole attack and explored a new concept that supports the network in various ways with detecting malicious activities of any node in the network and which will increases the network performance in parameters such as packet drop rate, throughput, normalized routing overhead and PDR

Keywords: *MANETS, DSDV, Security Threats, Gray hole Attacks, Routing Protocols, SEAD, S-DSDV*

1. INTRODUCTION

Wireless Mess Network technology has been touted as the 'last mile' in ubiquitous broadband Internet Access, it gives coverage as a cellular network and allows ease of use like a Wi-Fi network. The fact that it has already been tried and tested in practice, even before the 802.11s ESS (Extended Service Set) Mesh network specification has become a standard, makes it an attractive and approachable technology. WMNs have their roots in various previous tried and tested technologies like IEEE 802.11,MANETs, Wi-Fi networks etc. and are being developed to extend the mesh of technologies with WiMax networks (802.16), Sensor networks (IEEE 802.15.4), cellular networks, etc. WMNs are also popular due to their low cost, and ease of deployment. Depending on their architecture, a WMN can be classified into 3 types:

1) Infrastructure Mesh Networks: As opposed to an ad-hoc network or Wi-Fi network which has a flat topology, mesh networks have a hierarchical topology. As shown in Fig.1 dedicated mesh routers form an infrastructure for the clients. This meshing among the wireless routers creates a self-healing and self-configuring wireless communication system which provides each user, either fixed or mobile, with a high bandwidth, seamless, multi-hop interconnection service to other users and to the Internet via limited gateway connections or access points (also known in the WMN paradigm as mesh access points). The bridge functionalities in the routers allow integration with different types of networks.

2) Client Mesh Networks: These types of networks are similar to the conventional ad-hoc

Journal of Theoretical and Applied Information Technology
10th February 2016. Vol.84. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

networks. Here the end-users, either mobile or stationary, need to handle all configuration and routing functionalities.

3) ***Hybrid Mesh Networks:*** This is a combination of both of the earlier types. Here the routers connect myriad networks together, where improved connectivity and coverage is realized by the routing capabilities of the clients. Hence this architecture brings together all the advantages of WMNs. WMNs have interesting applications in broadband residential networking, military operations, disaster recovery, Intelligent Transportation Systems and Logistics, metropolitan area coverage, etc. Tempe, Arizona is the first city in the US to deploy a WMN blanketing the whole city with wireless accessibility.

Similar to WMNs, MANETs can also be classified according to their coverage area, e.g. LAN.WAN,PAN. Many routing protocols are used in MANETs which can be classified based on various criteria. Depend on routing the network topology will be changed that will be called as Table divan protocols or On Demand routing protocols. There are also hybrid protocols which combine both these features. If the network architecture and the role of the routing nodes are taken into account then the routing protocols can be grouped into a flat protocols. Routing Table driven protocol protocols sends as message/ packets topology information periodically and find routes to all nodes in a network, while reactive protocols find routes only . Whenever any node in the network want to communicate with the nodes then based on the performance analysis and experimental evaluation shows the reactive protocols outputs leads to form proactive routing protocols w.r.t. the pDR and routing overhead, and energy conservation. DSDV is a well-known proactive routing protocol. It works in the implicit 'trust your neighbor' mode in which all neighboring nodes are supposed to behave and work in tandem. The real world scenario though is completely different; any malicious user could destroy the network by manipulating the sequence numbers and routing messages. The problem could be further compounded by the dynamic changes caused in the WMN due to node mobility, error prone wireless channels, etc. The security needs of WMNs can be broadly classified into two types- security systems to protect 1) the data transmission or 2) securing the routing protocol messages.

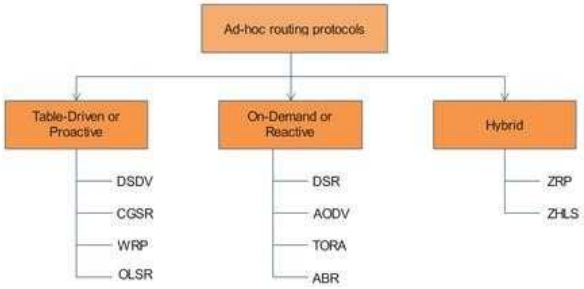

Fig no: 1 Ad-hoc Routing Protocols

2. DSDV OVERVIEW

This DSDV routing protocol is the routing table driven protocol which will be used in the MANETS. It consists of hop count as parameter in route selection. So DSDV is taken from RIP which is used in Ad hoc networks. By this to the network each will get one unique sequence number. This number will be used to distinguish the route path and duplication of packets will be avoided.

This DSDV routing protocol concentrated on the classical Bellman-Ford routing protocol which involves a concept of maintaining of routing information at the base station, like sequence number, number of hopping, etc, These nodes will also transmits the updated information also to the other nodes. By this nodes can easily detect the duplication of data packets then we can avoid the traffic on the nodes we can increase the throughput also.

Table No: 1 Routing Table of DSDV

Routing Table for Node 2

Destination	Next Hop	Metric	Dest. Seq. No.
1	1	1	123
2	0	0	516
3	3	1	212
4	4	1	168
5	4	2	372
8	1	INF	432

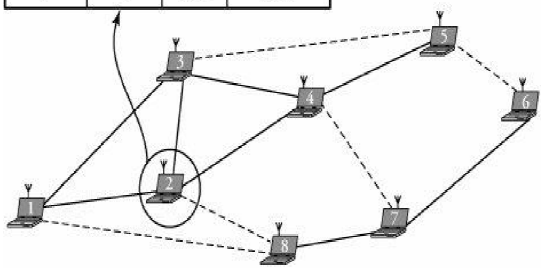

Figure No. 2 DSDV Routing Protocol

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. SECURITY CHALLENGES IN WMNET

Wireless mesh networks function as regular wireless networks, but with significant differences. Mesh networks decentralize the infrastructure required to maintain a network by making each node, or computer, pull double-duty as a user and a router of Internet traffic. This way, the network exists as an organic and self-managed entity capable of servicing a varying number of users. People joining or using wireless mesh networks for business purposes should be aware, however, that this interface isn't without security problems.

3.1. Physical Attacks

Internet access speeds up when more users contribute to the network, but it also opens up the network to multiple points of access. As all nodes in a WMF as routers, every node represents a possible point of attack. Computer nodes also can be compromised by the loss or theft of a laptop or desktop computer. In this case, the attacker stealing the computer can use the access provided by the stolen computer to enter the network, or simply disrupt the total system by removing of crucial routing based nodes.

3.2. Denial of Service

Even without physical access to the network, hackers can create "zombie" computers using virus infections. Once infected, each computer does the bidding of the attacker without direct monitoring. Meanwhile, the hacker launches a concentrated denial-of-service attack, which floods a particular computer or system with overwhelming bits of information to effectively shut down that system's ability to communicate with other networks. If a computer in a mesh network becomes infected, it can attack other computers inside its own network, and infect them as well, causing a cascading effect.

3.3. Passive Monitoring

A zombie computer doesn't need to attack the system to cause damage. Hidden and compromised computers can passively monitor Internet traffic moving through the network, giving the attacker the ability to intercept bank information, login credentials for any website accessed and routing information for the network itself. At this point, the attacker can chose to leave the network without anyone knowing, while possessing enough data to steal bank funds, commit identity fraud or re-enter the network at will.

3.4. Gray, Black and Wormholes

If a computer becomes infected or various computer enters into mesh network, and can be interpretend to be a trusted member of that network and then modify sent data and disrupt how the network passes information. In a black hole attack, information passing through the infected computer will not continue through the network, blocking the flow of data. In gray hole attacks, some data may be blocked, while other data is allowed, making it seem like the computer is still a working part of the network. Wormhole attacks are harder to detect: They tunnel into a network computer from the outside and pretend to be other nodes in the network, essentially becoming invisible nodes. They can then monitor network traffic as it passes from one node to the next.

4. TYPES OF SECURITY ATTACKS

Classes of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states. A system must be able to limit damage and recover rapidly when attacks occur.
There are five types of attack:

4.1. Passive Attack

A **passive attack** monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. **Passive attacks** include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

4.2. Active Attack

In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

4.3. Distributed Attack

A distributed attack requires that the adversary introduce code, such as a Trojan horse or back-door program, to a "trusted" component or software that will later be distributed to many other companies and users Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.

4.4. Insider Attack

An insider attack involves someone from the inside, such as a disgruntled employee, attacking the network Insider attacks can be malicious or no malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task

4.5. Close-in Attack

A close-in attack involves someone attempting to get physically close to network components, data, and systems in order to learn more about a network Close-in attacks consist of regular individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry into the network, open access, or both.

One popular form of close in attack is social engineering in a social engineering attack, the attacker compromises the network or system through social interaction with a person, through an e-mail message or phone. Various tricks can be used by the individual to revealing information about the security of company. The information that the victim reveals to the hacker would most likely be used in a subsequent attack to gain unauthorized access to a system or network.

5. GRAY HOLE ATTACK

In computer networking, a packet drop attack or black hole 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 lousy 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 t seconds, or a randomly selected portion of the packets. This is rather called a gray hole attack. If the malicious router attempts to drop all packets that come in, the attack can actually be discovered fairly quickly through common networking tools such as traceroute. Also, when other routers notice that the compromised router is dropping all traffic, they will generally begin to remove that router from their forwarding tables and eventually no traffic will flow to the attack. However, if the malicious router begins dropping packets on a specific time period or over every n packets, it is often harder to detect because some traffic still flows across the network.

The packet drop attack can be frequently deployed to attack wireless ad hoc networks. Because wireless networks have a much different architecture than that of a typical wired network, a host can broadcast that it has the shortest path towards a destination. By doing this, all traffic will be directed to the host that has been compromised, and the host is able to drop packets at will. Also over a mobile ad hoc network, hosts are specifically vulnerable to collaborative attacks where multiple hosts will become compromised and deceive the other hosts on the network.

6. IMPACT OF GRAY HOLE ATTACK

The performance of ad-hoc network decreases, When a Gray Hole attack takes place in the ad-hoc network. Gray Hole attack decreases certain performance metrics of the network such as packet delivery ratio, end to end delay & packet loss ratio.

1. **Packet delivery ratio (PDR):** It is ratio of packets sent from the source to packets received at the destination.

PDR =Ps/Pr

2. End to end delay (e2e): It refers to the time taken for a packet to be transmitted across a network from source to destination.

End to end delay D =Td-Ts

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. Packet loss ratio: It defines the packet dropped ratio when the network traffic fails to reach the destination in a timely manner.
Packet loss, Pd= Ps-Pa

Gray Hole attack can interrupt the network functionality at a higher level and can cause a great inconvenience to the users and it is also very difficult to detect such attack. So here in section, various detection and prevention methods for Gray Hole attack have been studied and compared with each other to find out an efficient and more secure method.

7. RELATED WORK OR EXISTING SOLUTIONS:

7.1 Using watchdog

In [1] malicious node can be detected using a watchdog timer. Every node monitors its next node in the route. If any packet forwarding misbehavior or any packet dropping in a predefined period of time for its next node is found, the next node is announced as a malicious node to the source.

Advantages

It is very simple method. One node need just listen to its next node in the route.

Disadvantages

Each node must monitor its next neighbor node.

Source node has to trust the other node's information about one node's misbehavior.

As there isn't any threshold value is used, it increases numbers of mistakes to find Gray Hole attacks.

7.2 Using SCAN approach

SCAN [2] makes use of two ideas to protect AODV in MANET as mentioned below:

Local collaboration: Basic idea behind this approach is that each node monitors each other and also sustains routing tables for each other. Every node has a token that provides authentication for the network. If one node is suspected to be malicious, other nodes revoke its token and alert token revocation to all nodes in network. Malicious node is inserted in token revocation list. So, the malicious node cannot have any access to the network.

Information cross-validation: Incoming routing packets checked by the each node.

As each node have all the information about its neighbors' routing table, it can crosscheck the overheard transmissions of them. Node M uses routing tables of X and Y, if X or Y announces a new fault routing update, M compares routing tables of two neighbors and if any misbehavior found, it announces that node as malicious to the network and revokes its token.

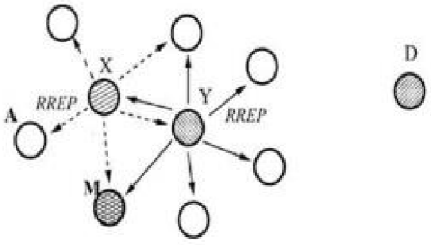

Fig No: 3 Cross-Checking Routing Updates Of Neighbors [10].

Advantages

A token is used which authenticates the node to the whole network. Without a valid token, a node cannot participate in the network and using token enhances the security of network to some extends.

Disadvantages

Mobility of nodes makes changes in routing tables which causes probable mistakes in finding malicious nodes. Also it is mandatory to update the table entry of neighbors in certain time periods.

7.3 Using Strong Nodes

In [3], a method is defines which uses some additional nodes, Strong nodes, which help source and destination to find Gray Hole attacks. These nodes are assumed to be trustful and also capable of tuning its antenna to large ranges as well as short ranges. Each normal node is within the range of one of these strong nodes. Strong nodes help the source and the destination nodes to perform an end-to-end check and get to know whether the data packets are reached to the destination or not. If any difference is found in number of messages sent from source and received in destination, strong nodes ask the nodes in their area about the monitoring results of one node's behavior. If the checking results show misbehavior according to the votes, then the backbone network runs a protocol which can detect black or Gray Hole attack. At the end announces malicious node to the network by broadcasting messages.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Advantages

Due to strong nodes ratio of monitoring of neighbors is decreased. Only nodes in particular area of malicious node have to monitor.

Disadvantages

Strong nodes are assumed to be trustable and there isn't any solution considered for attacks.

There is no threshold value for detection of maliciousness of one node which increases mistakes to distinguish between normal and strong nodes.

7.4 Detection using four reliable steps

The method introduced in [4] detects malicious nodes in four steps:

Data collection of neighbors: Each node collects information about all neighbors and stores it in its DRI table. If any neighbor node is found with from and through table fields with 0values then that node is assumed as a malicious node.

Local anomaly detection: Now source node selects a Cooperative Node (CN). This node contains both DRI fields filled with 1 value and is a trusted node as source previously sent to and received data from it. Source node broadcasts RREQ to CN as destination, then source asks to CN if it has received RREQ from malicious node, if it receives then source node removes that node from malicious nodes list as it does not drop RREQ packets. But if CN does not receive RREQ packet from malicious node, source node increases its maliciousness.

Cooperative anomaly detection: To avoid mistakes in malicious node detection, source node sends a cooperative detection request to all neighbors of malicious node. On receiving this request all neighbors send RREQ message through that node to source node as destination. That node returns RREP to neighbors. These neighbor nodes also sends a probe packet from malicious node to source and also another packet from another path to announce source about that packet, if source does not get probe packet. Until three times of sending probe packets by neighbors does not mark that node as Gray Hole attack and after three times marks that node as an attacker.

Global alarm sending: Finally, source node announces a node as a Gray Hole attacker.

Advantages

Nodes need not to monitor each other, so does not consume a lot of energy.

Three times of checks for a node increases surety and decreases mistakes.

Disadvantages

Increases the speed of distinguishing a Gray Hole attack increases and overhead for each malicious node detection is high.

7.5 Using Credit Based Technique

In this proposed approach [5], the AODV protocol is a little modified and a new algorithm is known as Credit Based AODV (CBAODV). In which, firstly each and every node assigns a permanent value for its every adjacent node as the neighbor credit value. This credit value is increases by the protocol when it receives a route request packet (RREQ) and decreases when it receives the route reply (RREP) packet. When a node finds negative credit value for one of its neighbors, then it detected as the gray hole attacker. [5] This also removes all current established paths from its routing table which is going through that node. Each node assigns accredit value that we are sending the route request and subtracting the credit value when we got a reply from them. This algorithm is capable to detect cooperative gray hole nodes. [5]

7.6 Using Signature attack

In [6], Gray Hole attack is implemented. Both the scenarios like with and without the presence of malicious nodes is implemented and packed delivery ratio is calculated for both scenarios. In the presence of malicious scenario, packet delivery ratio is comparatively less. Using an algorithm such malicious nodes can be identified. Simulations results are shown in two format i.e. one is NAM and the other is trace file. After simulation of both scenarios, we get two trace results from normal scenario and malicious scenario accordingly. Using these trace results a new detection algorithm is proposed which uses these two trace files to detect malicious node. The algorithm analyzes the data collected from both trace files. First trace file is for the normal scenario which defines legal behavior. In malicious scenario, some nodes are set as malicious. Now trace file behavior of these malicious nodes is compared with legal or normal behavior which defines a specific behavior pattern of Gray Hole attack for malicious node. This pattern is called signature of attack, which is used to detect malicious node. When user defines any scenario then its trace file is compared with previously created signature of attack. If the signature is matched with trace results of some nodes from user defined scenario then it declares those specific nodes as malicious. In this method, a main criterion for identification of a malicious node

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

is the creation of signature of attack from malicious scenario and it is compared with a normal scenario.

Advantages As we are already having a signature of attack, finding out misbehavior becomes very easy by comparing the signature of attack and trace file of user defined scenario.

Disadvantages We must have to implement both normal and malicious scenario to apply this approach.

8. PROPOSED APPROACH

Gray Hole attacks are very big security problems in MANET. Gray Hole attack drops packets in transmitting step. Detection of gray hole is more difficult because the attacker works as normal node then starts dropping of data. Smaller sequence number and longer distance frauds clearly violate the routing protocol specifications, and can be used for non-benevolent purposes. Although the damage they can cause has been thought less serious than those of larger sequence number fraud or shorter distance fraud, we believe they still need to be addressed for many reasons. Two of them are as follows: 1) they can be used by selfish nodes to avoid forwarding traffic, thus detecting these frauds would significantly reduce the means of being selfish; 2) it is always desirable to detect any violation of protocol specifications even though its damage may remain unclear or the probability of such violation seems low.

We use consistency checks to detect sequence number frauds and distance frauds in DSDV. Our Proposed mechanism has the following security properties, provided that no two nodes are in collusion: 1) detection of both larger and smaller sequence number fraud; 2) detection of any distance fraud. One feature is that a misbehaving node surrounded by well-behaved nodes can be contained. Thus, misinformation can be stopped in the first place before it spreads into a network. Our analysis shows that mechanism produces higher network overhead. However, it can be controlled by adjusting configurable parameters, like the intervals of consistency checks.

8.1 S-DSDV

In this, we present the complete details regarding S DSDV, which prevents any distance fraud, including longer, same, or shorter, shows that there are no two nodes in collusion.

8.2 Assumptions

This requires cryptographic functions for message authentication. Pair-wise shared keys or public key infrastructure to meet such requirement. we assume that each node in the network has a pair of public key and private key. Each node's public key in the network is certified by a trenty trusted by every node in the network. To reduce the computational overhead, every node in the network establishes a different secret key shared with every other node in the network. Combined with message authentication algorithms (e.g., MD5), pair-wise shared keys provide entity and message authentication. Thus, all messages in S-DSDV are cryptographically protected. If a routing protocol can scale from small to a large network it would be ideal without a limitation on its boundary. But, a distance vector routing protocol is usually used for a small or medium size network.

8.3 Review of S-DSDV

We assume r_u (w) = (w, seq (u,w), cst(u,w), nhp(u,w)), denotes the route from u to w where seq (u,w) denotes the sequence number of r_u (w),cst (u,w) denotes the cost of r_u(w) and nhp(u,w) denotes the next hop of $_{ru}$(w). With no vagueness, we also use (w,seq,cst), (w,seq,cst,nhp) , or (w,sequ,cstu,nhpu) to denote ru(w).

We classify routes R_u={r_u} advertisd by node u into two categories:

Those that u is authoritative of, denoted by R_u^{auth}; and

Those that u is unauthoritative of, denoted by R_u^{auth}.

$R_u = R_u^{auth} \cup R_u^{auth}$

Authoritative Routes: Given a route r_u=(w,seq,cst), ru ϵ R_u^{auth} if 1) w= u and cst = 0; or 2) cst =∞

Non-Authoritative Routes: Given a route r_u=(w,seq,cst), ru ϵ R_u^{auth} if w $\neq$ u and 0 < cst < ∞.

Validation of Authoritative Routes: If u is authoritative of r_u, a recipient node v validates the message authentication code (MAC) of r_u. If it succeeds, v accepts r_u. Otherwise, v drops r_u.

Validation of Non-Authoritative Routes: If u is unauthoritative of r_u, a recipient node v validates the data integrity of r_u. If it succeeds, v additionally validates the consistence of r_u. If it succeeds, v accepts r_u. Otherwise, v drops r_u.

Consistency:- Given a network G =(V,E), let u, v, w ϵ V and link e(u,w) ϵ E. for two routes r_u(w)=(w,seq(u,w), cst(u,w)), r_v(w)=(w,seq(v,w), cst(v,w)), and r_u(w) is directly computed from r_v(w). We say that r_u(w) and r_v(w) are **consistent** if

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1) seq(u,w)= seq(v,w); and 2) cst(u,w) = cst (v,w) + cst (u,v).

The following process illustrates how S-DSDV works: u,w∈V, u advertises a route r_u=(w,seq,cst,nhp) for w. Note r_u is protected by MAC.

Upon receiving from u, a route r_u,x∈V validates the MAC of the message carrying ru. If it fails, the message is dropped. Otherwise, x furher determines if u is authoritative of r_u. If yes, x accepts r_u. Otherwise, x checks the consistency of r_u with its next hop node (nhp), let's say v (see Step) 3). If it succeeds, r_u is accepted. Otherwise, it is dropped.

X uses to sends a route request to v (likely via u), asking r_u(w) and r_v(u), v should send back a route response containing its route entries for w and u. upon receiving r_v(w) and r_v(u), x can perform consistency check of r_u(w) and r_v(w) according to Definition 3. Note that u may manipulate x's route request and/or v's route response. However, such misbehavior will not go unnoticed since all message are MAC-protected.

9. CONCLUSIONS AND FUTURE WORK

In Many real time applications, secure routing is critical to the accept. The existing work done by different authors are very important in understanding the threat and in proposing an effective scheme for detecting and preventing the Gray Hole attack. Misbehavior of nodes may cause severe damage, even it fails the working whole of the network. In this paper, we have surveyed and presented the impact of gray hole attack and its consequences. Misbehavior of nodes causes the damage to the nodes & packet also. Gray hole attack cause damage to the network and also it is difficult to detect. Proposed approach can be integrated on the basic of routing protocol such as DSDV. Proposed mechanism detects the distance fraud and also detects both larger and smaller sequence number fraud. Thus, misinformation or misbehaving node can be stopped in the first place before it spreads into the network. To show the effectiveness and result of proposed approach, implementation work on Network Simulator 2 still in progress. Future works will include some mechanism so as to recognize & remove the gray hole attack.

REFRENCES:

[1] Mitigating Routing Misbehavior in Mobile Ad-hoc Networks by Sergio Marti, T.J.Giuli, Kevin Lai, Mary Baker, *Department of Computer Science*, *Stanford University, Stanford*, CA 94305 U.S.A.

[2] Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile AdHoc Networks by Sukla Banerjee, *Proceedings of the World Congress on Engineering and Computer Science* 2008, WCECS 2008, October 22 - 24, 2008, *San Francisco*, USA. ISBN: 978-988-98671-0-2

[3] Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad -hoc Networks by Shalini Jain, Mohit Jain,

[4] HimanshuKandwal, 2010 *International Journal of Computer Applications* (0975 – 8887)*Volume* 1 – No. 7 Methods of Preventing and Detecting Black/Gray Hole Attacks on AODVbased MANET by MarjanKuchaki Rafsanjani, Zahra ZahedAnvari and ShahlaGhasemi, *IJCA Special Issue on* "*Network Security and Cryptography*" NSC, 2011

[5] Deepali A.Lokare, A.MKanthe, Dina Simunic,"Cooperative Gray Hole Attack Discovery and Elimination using Credit based Technique in MANET", *International Journal of Computer Applications* (0975-8887), *Volume* 88No.15, pp. 13-22, February 2014

[6] Intrusion Detection System for AODV Protocol in MANET by Ms. S.R. Shirke, Prof. (Dr.) V. R. Ghorpade, *International Journal of Engineering Research & Technology (IJERT)* Vol. 2 *Issue* 5, *May* - 2013 ISSN: 2278-0181

[7] S. J. Patel et. al. "A Novel Approach to Gray-hole and Black-hole Attacks in Mobile Ad-hoc Networks" *Second International Conference on Advanced Computing & Communication Technologies*, 2012 IEEE, Pp 556-560.

[8] Onkar V. Chandure, V. T. Gaikwad, "Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol", *International Journal of Computer Applications*(0975-8887), Volume 41- No.5, pp. 27-32, March 2012.

[9] S. Jain, M. Jain, H. Kandwal, "Advanced algorithm for detection and prevention of cooperative Black and Gray hole attacks in mobile ad hoc networks", *IJCA* (0975-8887), Vol. 1-No. 7, pp. 37-42, 2010.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[10] M. Wahengbam and N. Marchang, "Intrusion Detection in MANET using Fuzzy Logic", *2012 IEEE*, Pp 456-460.

[11] R. H. Jhaveri, S. J. Patel, D. C. Jinwala, "A novel approach for Gray hole and Black hole attacks in Mobile Ad-hoc Networks", *Second International Conference on Advanced Computing & Communication Technologies, IEEE,* pp. 556-560, 2012.

[12] Jaydip sen et. al "A Mechanism for Detection of Gray Hole Attack in Mobile AD Hoc Networks" *ICICS* 2007, *IEEE*.

[13] Maha Abdelhaq et. al "A Local Intrusion Detection Routing Security over MANET Network" 2011 *International Conference on Electrical Engineering and Informatics,* 2011 *IEEE*

[14] Latha Tamilselvan and V. Sankaranarayanon "Prevention of Black hole Attack in MANET" *The 2nd International Conference on wireless Broadband and Ultra Wideband Communications*, 2007 *IEEE*.

[15] Y .C. Hu, D.B. Johnson, and A.Perrig. Secure Efficient Distance Vector Routing Protocol in Mobile wireless Ad Hoc Networks. *In Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications* (WMCSA 2002), *June* 2002

[16] Y .C. Hu, D.B. Johnson, and A.Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. *In Ad Hoc Networks Journal,* 1 (2003):175-192.

[17] Megha Arya, Yogendra Kumar Jain, "Gray hole Attack and Prevention in mobileAdhoc Network," *International Journal of Computer Applications* (0975 -8887), *Volume* 27– No.10, *August* 2011

[18] P. Agrawal, R. K. Ghosh and S. K. Das, "Cooperative black and gray hole attacks in mobile ad hoc networks", *In Proceedings of the 2nd International Conference on Ubiquitous Information Management and Communication*,pp.310-314,January-2008.

[19] Hizbullah Khattak, Nizamuddin, "A Hybrid Approach for Preventing Black and Gray Hole Attacks in MANET", *Digital Information Management (ICDIM) Eighth International Conference*, pp. 55-57, IEEE September 2013.

[20] Kamarularifin Abd Jalil et. al. "Securing Routing Table Update in AODV Routing Protocol" *IEEE conference on Open Systems*, 2011, IEEE, pp. 116-121.