A New Security Mechanism for Mitigating Multiple Grayhole Attack In MANETS

Shardha Jain
Department of Computer Science & Engineering
Ambala College of Engineering & Applied Research,
Devsthali, Ambala (Haryana)

Ashok Kajal
Department of Computer Science & Engineering
Ambala College of Engineering & Applied Research,
Devsthali, Ambala (Haryana)

Shanu Malhotra
Department of Computer Science & Engineering
ISTK, Yamuna nagar (Haryana)

Abstract

Wireless Ad hoc networks are temporary networks because they are formed to fulfil a special purpose and cease to exist after fulfilling this purpose. Mobile devices might arbitrarily leave or join the network at any time, thus ad hoc networks have a dynamic infrastructure. The number of applications that involve wireless communications among mobile devices is rapidly growing. Many of these applications require the wireless network to be spontaneously formed by the participating mobile devices themselves. In wireless ad hoc networks, mobile nodes communicate with other nodes over wireless links, without the support of pre-existing infrastructures, which is an attractive form of peer communications for certain applications. Providing entity authentication and authenticated key exchange among nodes are both target objectives in securing ad hoc networks. With the emergence of more heterogeneous devices and diverse networks, it is difficult, if not impossible, to use a one-size-fits-all encryption algorithm that always has the best performance in such a dynamic environment. Network security plays a crucial role in this MANET and the traditional way of protecting the networks through firewalls and encryption software is no longer effective and sufficient. In this paper, We have studied the effect of gray hole attack in the Ad hoc Networks and proposed solution that tries to eliminate the gray hole effect by monitoring scheme to isolate malicious node from the network over AODV routing protocol through simulatuion using ns2 simulator.

Keywords: QoS, AODV, MANETs

I. INTRODUCTION

With the rapid advance of miniaturized computers and radio communication technologies, wireless ad hoc networks have attracted a lot of attention from both research communities and the industry in recent years ; without relying on any pre-existing communication and computing infrastructures, autonomous peers are envisioned to communicate with other peers over wireless links, or to assist communications among others when necessary. Also, mobile peers can join or leave such systems at any time; when peers are in these systems, they can change their location at any time. This self-organizing and adaptive form of peer communications is particularly attractive in certain scenarios, where communication or computing infrastructures are either too expensive to build or too fragile to maintain. Wireless ad hoc networks have found any applications in military, commercial and consumer domains; they also have other variants (e.g., wireless sensor networks) with various similarities. Due to the absence of properly-protected media and well-trusted infrastructures, and due to the reliance on unknown third-parties to relay data, peer communications in these systems are intrinsically vulnerable to various passive and active attacks , which can compromise the confidentiality, integrity and authenticity of information exchange among peers. Also, in some wireless ad hoc networks, peers can become selfish, greedy and even tampered by adversaries, which brings more challenges to secure the already vulnerable peer communications in these systems. Many efforts have been devoted to securing peer communications in wireless ad hoc networks, and most of them are based on either symmetric-key or public key cryptography. Although these systems have successfully demonstrated their capability in securing information infrastructures (e.g., the Internet), many of them are found inadequate for wireless ad hoc networks, either due to severe communication or computing constraints, or due to the lack of infrastructure support in such networks.

Mobile Ad hoc wireless networks are self-creating, self-organizing, and self-administering. They come into being solely by interactions among their constituent wireless nodes, and it is only such interactions that are used to provide the necessary administration functions supporting such networks.

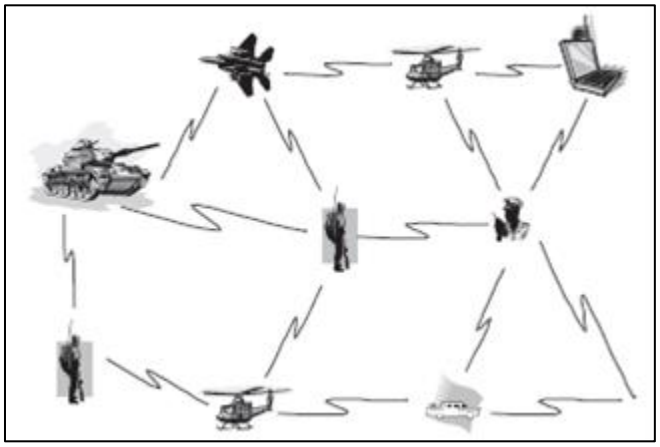


Fig. 1: Mobile Ad hoc Networks

Mobile ad-hoc networks offer unique versatility for certain environments and certain applications. Since no fixed infrastructure, including base stations, is prerequisite, they can be created and used any time, anywhere. Indeed, since all nodes are allowed to be mobile, the composition of such networks is necessarily time varying. Addition and deletion of nodes occur only by interactions with other nodes; no other agency is involved. Such perceived advantages elicited immediate interest in the early days among military, and rescue agencies in the use of such networks, especially under disorganized or hostile environments, including isolated scenes of natural disaster and armed conflict.

Security is an essential service for wired and wireless network communications. The success of MANET strongly depends on whether its security can be trusted. However, the characteristics of MANETpose both challenges and opportunities in achieving the security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation.

A. Security Issues and Challenges:

The special properties of ad hoc networks enable all the neat features such networks have to offer, but at the same time, those properties make implementing security protocols a very challenging task. One of the fundamental vulnerabilities of MANETs comes from their open peer-to-peer architecture. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. As a result, there is no clear line of defense in MANETs from the security design perspective. The boundary that separates the inside network from the outside world becomes blurred. There is no well-defined place or infrastructure where we may deploy a single security solution. There are four main security problems that need to be dealt with in ad hoc networks:

1) The authentication of devices that wish to talk to each other;
2) The secure key establishment of a session key among authenticated devices;
3) The secure routing in multi-hop networks; and
4) The secure storage of (key)data in the devices.

B. Security Attacks:

Security attacks can be classified in different ways. One way is to divide attacks into four categories according to where the attacker deploys the attack in the flow of information from a source to a destination.

1) Interruption: An asset of the network is destroyed or becomes unavailable or unusable. This is an attack on availability. Examples include silently discarding control or data packets.
2) Interception: An unauthorized node gains access to an asset of the network. This is an attack on confidentiality. Examples include eavesdropping control or data packets in the networks.
3) Modification: An unauthorized node not only gains access to but tampers with an asset. This is an attack on integrity. Examples include modifying control or data packets.
4) Fabrication: An unauthorized node inserts counterfeit objects into the system. This is an attack on authenticity. Examples include inserting false routing messages into the network or impersonating other node.
   A more useful categorization of these attacks is in terms of passive attacks and active attacks :
5) Passive attacks: A passive attack does not disrupt the operations of a routing protocol, but only attempts to discover valuable information by eavesdropping, or silently discard messages received. Three types of passive attacks are release of message contents, traffic analysis, and message dropping.
6) Active attacks: An active attack involves modification of the contents of messages or creation of false messages. It can be subdivided into four categories masquerade, replay, modification of messages, and denial of service.

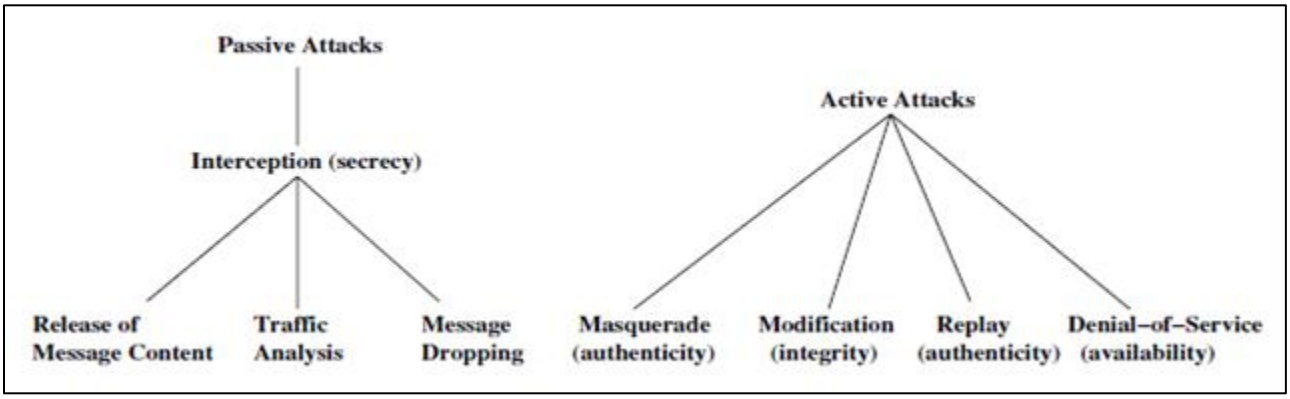


Fig. 2: Categorization of Attacks

C. Security Mechanisms:

A variety of security mechanisms have been invented to counter malicious attacks. The conventional approaches such as authentication, access control, encryption, and digital signature provide a first line of defense. As a second line of defense, intrusion detection systems and cooperation enforcement mechanisms implemented in MANET can also help to defend against attacks or enforce cooperation, reducing selfish node behavior.

1) Preventive Mechanism:

The conventional authentication and encryption schemes are based on cryptography, which includes asymmetric and symmetric cryptography. Cryptographic primitives such as hash functions (message digests) can be used to enhance data integrity in transmission as well. Threshold cryptography can be used to hide data by dividing it into a number of shares. Digital signatures can be used to achieve data integrity and authentication services as well. It is also necessary to consider the physical safety of mobile devices, since the hosts are normally small devices, which are physically vulnerable. For example, a device could easily be stolen, lost, or damaged. In the battlefield they are at risk of being hijacked. The protection of the sensitive data on a physical device can be enforced by some security modules, such as tokens or a smart card that is accessible through PIN, passphrases, or biometrics. Although all of these cryptographic primitives combined can prevent most attacks in theory, in reality, due to the design, implementation, or selection of protocols and physical device restrictions, there are still a number of malicious attacks bypassing prevention mechanisms.

2) Reactive Mechanism:

An intrusion detection system is a second line of defense. There are widely used to detect misuse and anomalies. A misuse detection system attempts to define improper behavior based on the patterns of well-known attacks, but it lacks the ability to detect any attacks that were not considered during the creation of the patterns; Anomaly detection attempts to define normal or expected behavior statistically. It collects data from legitimate user behavior over a period of time, and then statistical tests are applied to determine anomalous behavior with a high level of confidence. In practice, both approaches can be combined to be more effective against attacks. Some intrusion detection systems for MANET have been proposed in recent research papers.

II. RELATED WORK

Jaydip Sen et al. [1], proposed a security mechanism is to defend against a cooperative gray hole attack for AODV routing protocol in mobile Ad hoc environment. The proposed security mechanism increases the reliability of detection by proactively invoking a collaborative and distributed algorithm involving the neighbour nodes of a malicious gray hole node. The proposed mechanism involves both local and cooperative detection to identify any malicious gray hole node in the network. Once a node is detected to be really malicious, the scheme has a notification mechanism for sending messages to all the nodes that are not yet suspected to be malicious, so that the malicious node can be isolated and not allowed to use any network resources. The mechanism consists of four security procedures which are invoked sequentially. The security procedures are Neighborhood data collection, Local anomaly detection, Cooperative anomaly detection, and Global alarm raiser. From simulation results, the authors show that the proposed mechanism is effective and efficient with high detection rate and very low false positive rate and control overhead.

Vinh Hoa LA et al. [2], presents a survey of VANETs attacks and their solutions Risks caused by security attacks are one of the major security issues for the VANETs that are constraining the deployment of the vehicular ad hoc networks. The authors presented an upto- date collection of attacks damaging VANETs, sampled the practical scenarios and also discussed the existing solutions to deal with attacks, and characterized each attack to have a thorough look over it. The authors conclude intruder detection as the better mechanism and intend to construct an intrusion detector for VANETs to alert the attacks in the case performing.

Bhimsingh Bohara et al. [3], discuss the effect of gray hole attack and their counter measuring solution over mobile adhoc network. The Grayhole attack is an active kind of attack on adhoc networks where the attacking node first forwards packets and then later on drops the packets resulting in Denial of Service (DoS). The author use Intrusion Detection scheme to report violation of policy and the nodes whose packets are dropped again try to establish new paths using Route Requests messages. The Gray hole attack is in a way bit similar to Black hole attack. A black hole attack where drops all the packets, on the other hand the gray hole attacking node drops packet with certain probability. The authors analyzed the effects of gray hole in an AODV network. From simulation results with varying speed and 30 nodes for normal AODV as well as after the inclusion of gray hole in AODV.

D.M. Shila et al [4] offered a solution to defend selective forwarding attack (gray hole attack) in Wireless Mesh Networks. The first stage of the algorithm is Counter- Threshold Based and uses the detection threshold and packet counter to discover the attacks. The second stage is Query- Based and uses acknowledgment from the intermediate nodes to confine the attacker. In the first stage, two types of packets, Control packet and Control ACK packet, are used to detect the attacker. Furthermore, they determine the proper value of detection threshold based on the routing Expected Transmission Count metric ETX to improve the performance under different network situation.

Sun et al. [5], presented a general approach for detecting the black hole attack. They planned a neighborhoodbased method to detect the interloper and a routing recovery protocol to set up a correct course to the true destination. They first introduced the neighbour set of a node, which is all of the nodes that are within the radio transmission range of a node. Two types of control packets are introduced to share neighbour set between different nodes. If two neighbour sets received at the same time are different enough, it can be accomplished that they are generated by two different nodes. One disadvantage of this scheme is that there must be a public key infrastructure or the detection is still susceptible.

Patcha et al. [6], proposed a collaborative method for black hole attack prevention. A watchdog method is introduced to include a collaborative architecture to deal with collusion amongst nodes. In this algorithm, nodes in the network are classified into trusted, watchdog, and ordinary nodes. Every watchdog that is chosen should observe its normal node neighbours and decide whether they can be treated as trusted or malicious.

Onkar V.Chandure et al. [7], describe the basic idea related with the implementation of AODV protocol and evaluates the impact of gray hole attack on adhoc network. A Gray hole is a node that selectively drops and forwards data packets after advertises itself as having the shortest path to the destination node in response to a route request message. The authors analyse the impact of gray hole attack on adhoc network for different performance metrices like packet delivery ratio and end to end delay. Simulation of AODV as well as gray hole attack is carried out by using ns-2 simulator.

Chetan S. Dhamande et al. [8], presented a brief study on different for the minimizing the impact of gray hole attack using AODV routing protocol.. Gray hole attack ultimately decrease the performance of the network & also corrupt the data Proposed solution is mainly focus on the miminize the impact of gray hole attack in MANET & also improve the security as well as the performance of the network. A gray hole may exhibit its malicious behavior in different ways. It may drop packets coming from or destined to certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of gray hole node may behave maliciously for Some time duration by dropping packets but may switch to normal behaviour later.

Tarun Varshney et al. [9], investigate more existing mechanisms to prevent blackhole attack and propose a slight modification to AODV, called Watchdog –AODV (WAODV) that detects blackhole attack and also attempt to reduce further rise in normalized routing overhead. This mechanism firstly detects a blackhole node and provide a new route to source node. This mechanism greatly increases reliability of detection and isolation of multiple malicious blackhole nodes during route discovery process and discovers a short and secure route towards destination without introducing additional control packets.

In cryptographic approaches like S-AODV [10] and Adriane [11], the routing packets are encrypted using symmetric or asymmetric algorithm and hence external or inside attacker cannot modify the packets. However the problem with cryptographic approaches is the increased consumption of processing power and flooding attack can also be launched without forging the packets.

In [12] Dahill, et al. proposed ARAN, a routing protocol for ad hoc networks that uses authentication and requires the use of a trusted certificate server. In ARAN end-to-end authentication is achieved by the source by having it verify that the intended destination was reached. In this process, the source trusts the destination to choose the return path. The source begins route instantiation by broadcasting a Route Discovery Packet (RDP) that is digitally signed by the source. Following this, every intermediate node verifies the integrity of the packet received by verifying the signature. The first intermediate node appends its own signature encapsulated over the signed packet that it received from the source. All subsequent intermediate nodes remove the signature of their predecessors, verify it and then append their signature to the packet.

One primitive solution to vanish the RREP forging is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node [13]. This method avoid intermediate node to reply which avoid in certain case the Black Hole and implements the secure protocol. This increase the routing delay in large networks and a malicious node can take advantage by replying message instead of destination node. So for this one or more routes are used by the intermediate nodes which replay the RREQ messages to confirm the routes from intermediate nodes and destination nodes for sending out the data packets. In case if it does not exist, the reply messages is discarded from intermediate node and alarm messages are sent to the network. This method avoids the Black Hole problem thus preventing the network from malicious node. This will result in great delay especially in large networks and in addition the attacker can fabricate a reply message on behalf of the destination node.

III. PROPOSED METHODOLOGY

Mobile Ad hoc Networks (MANET) is new paradigm of wireless networks providing unrestricted mobility to nodes with no fixed or centralized infrastructure. Each node participating in the network acts as router to route the data from source to destination. This characteristic makes MANET more vulnerable to routingattacks. A number of mechanism were proposed to solve the Grayhole problem. It requires a source node that initiates a checking procedure to determine the reliability of any intermediate node claiming that it has a fresh enough route to the destination. In this thesis, the behavior of grayhole attack and the performance impact of this attack on AODV protocol and its counter measures using Watchdog AODV scheme is studied. A reactive scheme is proposed that can identify the misbehaving node without causing much overhead. The NS2 network simulator is used for evaluation. This simulation process considered a wireless network of nodes which are placed within a 1400m X 1400m area. CBR (constant bit rate) traffic is generated among the nodes. The simulation runs for 100 seconds. Pause time is the time for which mobile nodes wait at a destination before moving to other destination. Low pause time signifies high mobility as the node will have to wait for lesser time duration. Keeping all other parameters constant, pause time is varied to observe the behavior of performance metrics.

Table – 1
Important Simulation Parameters

Parameter	*Value*
Simulation area	*1400m x 400m*
Antenna	*Omni antenna*
No. of nodes	*30*
Pause Time (sec)	*10, 15, 20, 25, 30*
Traffic	*CBR (Constant bit rate)*
Routing protocol	*AODV,*
Security attack	*GrayHole attack*
Security Mechanism	*Watchdog AODV*

Simulations are performed for Gray hole attack in a multi hop ad hoc network environment. The impact of node's mean pause time on the performance of AODV routing protocol under Gray hole security attacks is shown with the help of simulation graphs in terms of throughput, number of packet drops, packet delivery ratio, average end-to-end delay and routing load.

A. Throughput:

The figure 3 shows the effect of grayhole attack on the throughput of AODV and its prevention using Watchdog for different pause time.

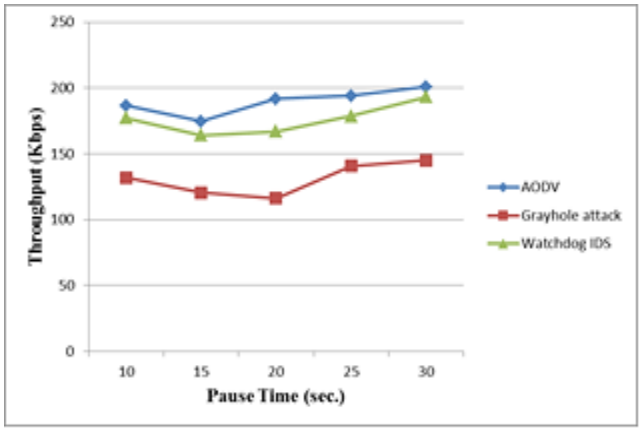
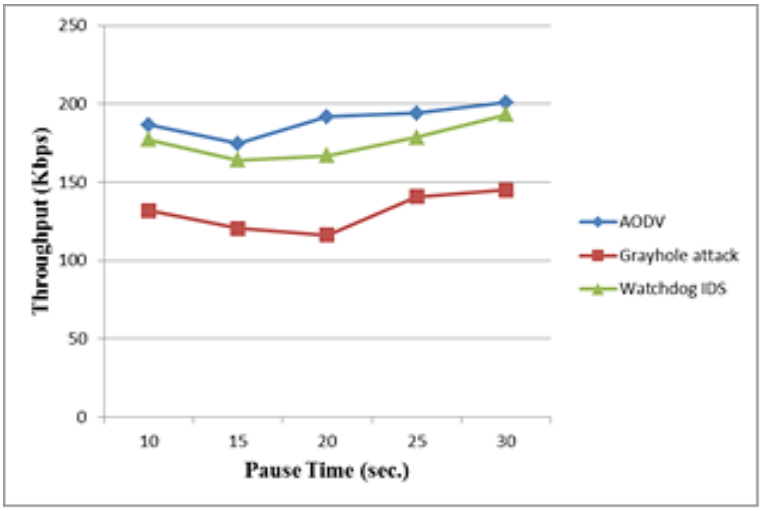


Fig. 3: Throughput of of AODV under grayhole and its counter measuring technique Watchdog IDS

The figure depicts that throughput of AODV routing protocol is heavily affected by grayhole attack. From the simulation reslts, we can see that Intruder detection system namely Watchdog IDS heavily reduces the effect of grayhole attack.



B. Packet Delivery Fraction:

Figure 4 shows the packet delivery ratio when the pause time is varied. The figure depicts that PDR of AODV routing protocol is heavily affected by grayhole attack attack. It has been observed from the simulation scripts that when the protocols are under attack of gray hole attack, watchdog-AODV has a more packet delivery ratio, as compared to AODV routing protocol under gray hole attack.

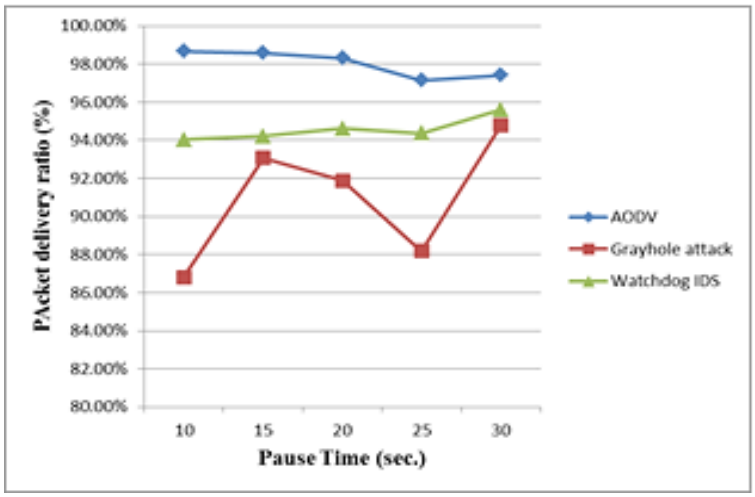


Fig. 4: PDF of of AODV under grayhole and its counter measuring technique Watchdog IDS

C. Average Delay:

Figure 5 shows the average end to end delay when the pause time is varied.

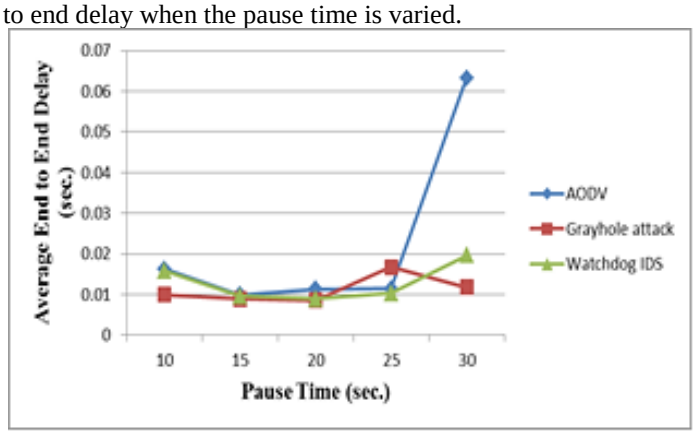


Fig. 5: Average delay of AODV under grayhole and its counter measuring technique Watchdog IDS

The figure depicts that average delay of Watchdog AODV routing under grayhole attack has better Average end to end delay as compare to AODV under attack.

D. Number of Packet Drops:

Figure 6 shows the amount of packet drops when the pause time is varied.The figure depicts that packet drops decrease in the case of Watchdog AODV routing under grayhole attack as compare to AODV under attack.

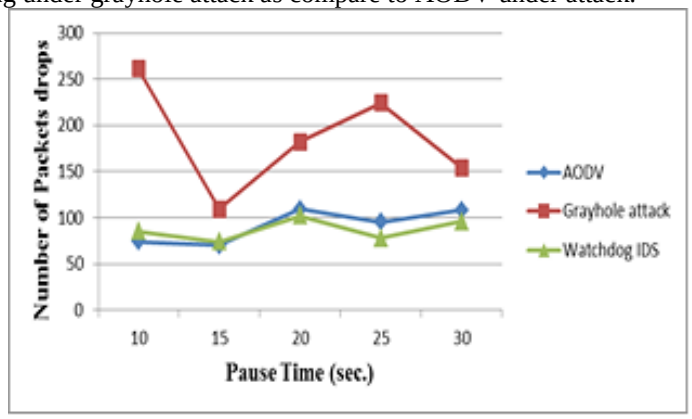


Fig. 6: Packet drops of AODV under grayhole and its counter measuring technique Watchdog IDS

E. Routing Overhead:

Figure 7 shows the routing overhead when the pause time is varied.The figure depicts that routing overhead decrease in the case of Watchdog AODV routing under grayhole attack as compare to AODV under attack.

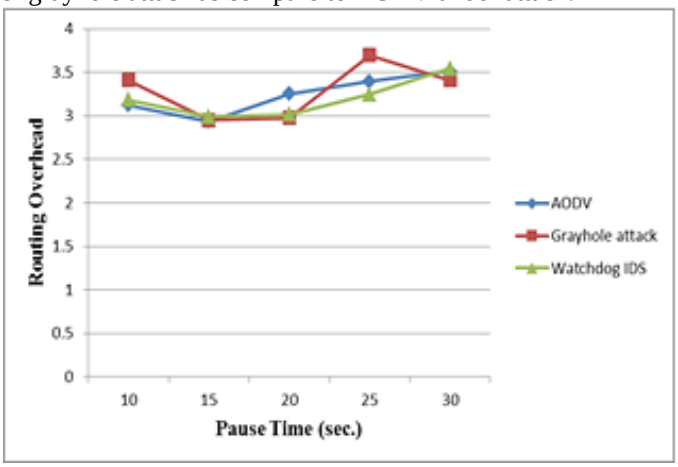


Fig. 7: Routing overhead of AODV under grayhole and its counter measuring technique Watchdog IDS

IV. CONCLUSION AND FUTURE WORK

In this paper, we simulated the gray hole attack in the Ad-hoc Networks and investigated its affects. Having simulated the grayhole attack, we saw that the performance of AODV is decreased in the ad-hoc network. Although many solutions have been proposed but still these solutions are not perfect in terms of effectiveness and efficiency. If any solution works well in the presence of single malicious node, it cannot be applicable in case of multiple malicious nodes. Our proposed solution tries to eliminate the gray hole effect by monitoring schemeto isolate malicious node from the network. The watchdog does this by listening to all nodes within transmission range promiscuously. If a watchdog detects that a packet is not forwarded within a certain period or is forwarded but altered by its neighbour it deems the neighbour as misbehaving and if any node only accept the node and does not forwarded, watchdog declare that node as a gray hole node and exclude that node from the path of the sending packets.

REFERENCES

[1] Jaydip Sen, M. Girish Chandra, Harihara S.G. and Harish Reddy, P. Balamuralidhar "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks" ICICS, IEEE, 2007.

[2] Vinh Hoa LA and Ana Cavalli " Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey" International Journal on Ad, Hoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014.
[3] Bhimsingh Bohara, Varun Sharma "Analysis and Prevention of effects of gray hole attacks on Routing Protocol in Mobile Ad-hoc Networks" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 6, June 2013.
[4] D.M. Shila, T. Anjali "Defending selective forwarding attacks in WMNs" International Conference on Electro/Information Technology, IEEE, 2008.
[5] B. Sun, Y. Guan, J. Chen, U.W. Pooch, "Detecting Black-hole Attack in Mobile Ad Hoc Networks" 5th European Personal Mobile Communications Conference, 2003.
[6] Patcha, A. Mishra "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks" Radio and Wireless Conference, IEEE, 2003.
[7] 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, Volume 41, issue 5 , March 2012.
[8] Chetan S. Dhamande, H. R. Deshmukh "A Efficient Way To Minimize the Impact of Gray Hole Attack in Adhoc Network" International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 2, February 2012.
[9] Tarun Varshney, Tushar Sharmaa, Pankaj Sharma "Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network" Fourth International Conference on Communication Systems and Network Technologies, IEEE, Oct. 2014, pp 217-221.
[10] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009.
[11] S. Yi and R. Kravets, Composite Key Management for AdHocNetworks.Proc. Of the 1st Annual InternationalConference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04), pp. 52-61, 2004.
[12] Hu, Y., Perrig, A., & Johnson, D. (2002). Ariadne: A Secure On-Demand Routing for Ad Hoc Networks. Proc. of MobiCom 2002, Atlanta
[13] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding Royer, "Secure routing protocol for Ad-Hoc networks," In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Comput. Sci., California Univ., Santa Barbara, CA, USA. Pp.78- 87, ISSN: 1092-1648, 12-15 Nov. 2002.