www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-1, Issue-4, Oct- 2013
Review Paper

Int. J. Sci. Res. in
Network Security
and Communication
ISSN: 2321-3256

Investigation Based Performance of Black and Gray Hole Attack in Mobile Ad-Hoc Network

Pradeep Kumar Sharma[1], Shivlal Mewada[2] and Pratiksha Nigam[3*]

[1,2,3*] *Department of Computer Science, Govt. Holkar Science College, Indore, India*

Received: 18 September 2013 Revised: 25 September 2013 Accepted: 16 October 2013 Published: 30 October 2013

Abstract- Mobile ad hoc networks (MANETs) are a set of mobile nodes which are self-configuring and connected by wireless links automatically as per the defined routing protocol. Security is an essential requirement in MANETs. Compared to wired networks, MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority and limited resources. Attacks on ad-hoc networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not. These mobile nodes communicate with each other without any infrastructure, furthermore, all of the transmission links are established through wireless medium. There is no guarantee that a communication path is free from malicious or compromised nodes which deliberately wish to disrupt the network communication. So protecting the mobile ad-hoc network from malicious attacks is very important and challenging issue. In this paper we address the study of different types of attack, problem of packet forwarding misbehavior and propose a mechanism to detect the black and gray hole attacks.

Key Words- Mobile Ad Hoc Network, Black Hole , Gray Hole

I. INTRODUCTION

Mobile Ad-Hoc network is an autonomous system, where nodes/stations are connected with each other through wireless links. There is no restriction on the nodes to join or leave the network, therefore the nodes join or leave freely. Mobile Ad-Hoc network topology is dynamic that can change rapidly because the nodes move freely and can organize themselves randomly. This property of the nodes makes the mobile Ad-Hoc networks unpredictable from the point of view of scalability and topology[1].

Mobile Adhoc Networks (MANETs) are dynamic in nature. Any nodes can join and leave the network at any time. Hence any type of intruders can attack the communication at any time, especially the routing mechanism between the nodes. In this study, we study and understand two types of attacks which cause more damage to the routing performance of MANET; the attacks are Black Hole attacks and Gray Hole attacks.[3]

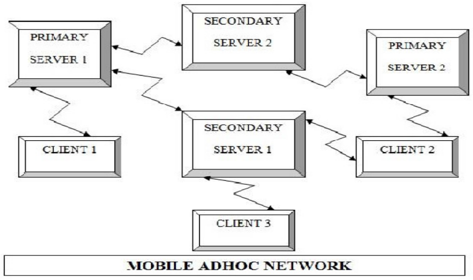

Figure 1 -Architecture of MANET [3]

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR [1].

Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats.

Corresponding Author: *Pratiksha Nigam*

The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication [2,4]. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

II. Related Work

Security is an essential requirement in mobile ad hoc network (MANETs). Compared to wired networks, MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority and limited resources. Attacks on ad hoc networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not. In this paper, we are describing the all prominent attacks described in literature in a consistent manner to provide a concise comparison on attack types [1]. To the best of our knowledge, this is the first paper that studies all the existing attacks on MANETs.

Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. It’s an analogy to the black hole in the universe in which things disappear. The node presents itself in such a way to the node that it can attack other nodes and networks knowing that it has the shortest path. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue.[2] In order to provide secure communication and transmission, researcher worked specifically on the security issues in MANETs, and many secure routing protocols and security measures within the networks were proposed.

Previously the works done on security issues in MANET were based on reactive routing protocol like Ad-Hoc On Demand Distance Vector (AODV). Different kinds of attacks were studied, and their effects were elaborated by stating how these attacks disrupt the performance of MANET.

The scope of this thesis is to study the effects of Black hole attack in MANET using both Proactive routing protocol i.e. Optimized Link State Routing (OLSR) and Reactive routing protocol Ad-Hoc On Demand Distance Vector (AODV). Comparative analysis of Black Hole attack for both protocols is taken into account. The impact of Black Hole attack on the performance of MANET is evaluated finding out which protocol is more vulnerable to the attack and how much is the impact of the attack on both protocols. The measurements were taken in the light of throughput, end-to-end delay and network load. Simulation is done in Optimized Network Engineering Tool (OPNET).

AODV: AODV is described in RFC 3561 [4]. It’s reactive protocol, when a node wishes to start transmission with another node in the network to which it has no route; AODV will provide topology information for the node. AODV use control messages to find a route to the destination node in the network. There are three types of control messages in AODV which are discussed bellow.

Request Message (RREQ): Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

Route Reply Message (RREP): A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

Route Error Message (RERR): Every node in the network keeps monitoring the link status to its neighbor’s nodes during active routes. When the node detects a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is down. Black hole attack disturbs the routing protocol by deceiving other nodes about the routing information. A black hole node works in the following scheme: once receiving RREQ and RREP messages, the attacker replies RREP messages directly and claims that it is the destination node. The source node is likely to receive a pseudo-RREP from the attacker before the real RREP returns. Under these circumstances, the source node sends data packets to the black hole instead of the destination node. When the source node transmits data packets through the black hole, the attacker discards them without sending back a RERR message. As for gray hole, its behavior is similar to a black hole. A gray hole does not drop all data packets but just part of packets. We define the *Gray Magnitude* as the percentage of the packets which are maliciously dropped by an attacker. For example, a gray hole is gray magnitude of 60% will drop a data packet with a probability of 60% and a classical black hole has a gray magnitude of 100%. The black and gray hole attack will bring great harm to the performance of Ad Hoc network. In previous research, the authors have carried out experiment on black hole attacks [6]. In Section V of this paper, we first analyze the impact of gray hole under different malicious drop rate. The malicious drop rate is defined by the ratio of dropped packet number and received packet number. Especially, the malicious drop rate of a black hole is 100%.

Previously the works done on MANETs focused mainly on different security threats and attacks. Among these attacks Black Hole attack involved in MANET is evaluated based on reactive routing protocol like Ad-Hoc On Demand Distance Vector (AODV) and its effects are elaborated by stating how this attack disrupt the performance of MANET. Very little attention has been given to the fact to study the impact of Black Hole attack in MANET using both Reactive and Proactive protocols and to compare the vulnerability of both these protocols against the attack. There is a need to address both these types of protocols under the attack, as well as the impacts of the attacks on the MANETs. This thesis analyzes Black Hole attack in MANETs using AODV and OLSR which are reactive and proactive respectively in nature.

III. OBJECTIVE OF THE STUDY

Previously the works done on MANETs focused mainly on different security threats and attacks. Among these attacks Black Hole attack involved in MANET is evaluated based on reactive routing protocol like Ad-Hoc On Demand Distance Vector (AODV) and its effects are elaborated by stating how this attack disrupt the performance of MANET. Very little attention has been given to the fact to study the impact of Black Hole attack in MANET using both Reactive and Proactive protocols and to compare the vulnerability of both these protocols against the attack. There is a need to address both these types of protocols under the attack, as well as the impacts of the attacks on the MANETs. The main Objective of this paper is to find out the solution for Black and Gray Hole Attacks.

IV. METHOD & PROPOSED CONCEPT

After whole research work I analyzed that all the attacks are raised due to the lack of centralized system. So if we link a centralized system with MANET then it prevent the attacks .It is a type of network where all users connect to a central server, which is the acting agent for all communications. This server would store both the communications and the user account information. Most public instant messaging platforms use a centralized network. Also called centralized server-structure

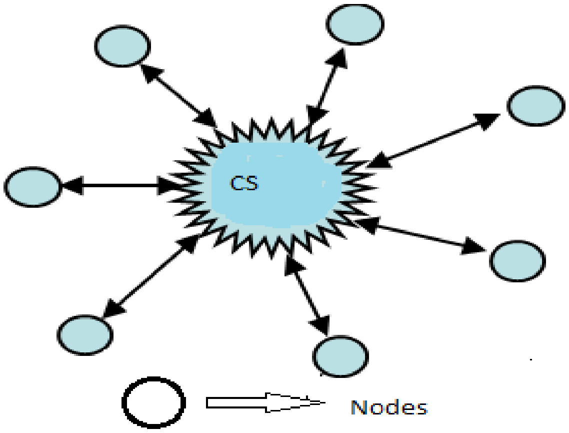

Fig 2: MANET with Centralized System

Advantage-

- It Maintains the record of malicious nodes
- It protect from Attacks to MANET. Because data will transmit through centralized system.

Disadvantage-

- It is a Time Consuming Process.
- If the System fails to work or down, then no transmission b/w MANET is possible.
- The initial costs are higher than with decentralized systems because you first have to invest in the master controller, which is generally the most expensive component of the installation.

V. CONCLUSION

In this study we have studied and analyzed the performance of two types of attacks known as Black Hole and Gray Hole attacks. As shown in graphs the impacts of these two attacks are considered under various network attributes and we have also compared the impact of these two attacks. As shown in the gray tables the Black Hole attacks are more vulnerable than Gray Hole attacks because the packet drop ratio is high for Black Hole attacks compared to Gray Hole attacks, not only that the normalized routing load also increases in the presence of Black Hole attacks compared to Gray Hole attacks.

When compared to packet delivery fraction Black Hole attacks delivery rate decreases compared to Gray Hole attacks, the routing packets also decreased in the presence of Black Hole attacks to that of Gray Hole attacks. In our future work we try to analyze other such types of malicious behavior in AODV protocol. Further, while studying the

AODV protocol we understand about its drawback, so we will provide a solution to secure AODV protocol.

VI. Future Work

Future work could-

- Design an algorithm for Centralized MANET.
- To overcome disadvantages of Centralized MANET.

References

[1] Umesh Kumar Singh, Shivlal Mewada, Lokesh Laddhani & Kamal Bunkar,"an Overview & Study of Security Issues in Mobile Adhoc Networks",Int. Journal of Computer Science and Information Security (IJCSIS) USA, Volume-9, No.4, pp (106-111), April **2011.**

[2] Shivlal Mewada and Umesh Kumar Singh, "Measurement Based Performance of Reactive and Proactive Routing Protocols in WMN", Int. Journal of advanced research in Computer Science and Software Engineering Vol. 1, No. 1, pp(1-4), Dec.-**2011**.

[3] C.E.Perkins and E.M.Royer, "Ad-Hoc On Demand Distance Vector Routing," Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applictions, pp.90-100, Feb, **2010**.

[4] Shivlal Mewada, Umesh Kumar Singh and Pradeep Kumar Sharma, " Simulation Based Performance Evaluation of Routing Protocols for Mobile Ad-hoc Networks (MANET)", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 2, No. 4,August **2012**

[5] M.Abolhasan, T.Wysocki, E.Dutkiewicz, " A Review of Routing Protocols for Mobile Ad-Hoc Networks," Telecommunication and Infromation Research Institute University of Wollongong, Australia, June, **2003.**

[6] T.Clausen, P.Jacquet , "Optimized Link State Routing Protocol (OLSR)", RFC 3626 October, **2003.**

[7] Z.J.Hass, M.R.Pearlman, P.Samar, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks", 55th Proceeding of International task force, July**, 2002.**

[8] P.V.Jani, "Security within Ad-Hoc Networks," Position Paper, PAMPAS Workshop, Sept. 16/17 **2002.**

[9] M.Parsons, P.Ebinger, "Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc networks",[Online].Available:www.cse.buffalo.edu/srds2009/dncms2009_submission_person.pdf, [Accessed: April. 10, **2010]**.

Authors Profile

Dr. Pradeep Sharma obtained his Ph.D. in Physics from Vikram University, Ujjain -INDIA. He is currently Professor and Head of department, (HOD) in Department of Computer Science, Govt. Holkar (Autonomous) Science College-INDIA. He has 29 year teaching experience in college level. His various research papers are published in national and international journals of repute. His various paper published in national and international conferences His research interest includes X-ray spectroscopy, Networking.

Shivlal Mewada has received his Master of Philosophy in Computer Science and He completed his Master of Science from Institute of Computer Science, Vikram University, Ujjain. He is currently pursuing Ph.D. in Computer Science from Institute of Computer Science, Vikram University, Ujjain. He is presently working as a lecturer in Department of Computer Science, Govt. Holkar Science Collage (HSC), Indore - India. He was awarded Junior Research Fellow Award by UGC New Delhi. He has published various research papers in international journals and international conferences. He shared the responsibility of research advisor (M.Phil.) in HSC Collage. He has co-supervised four M.Phil. and one M.Sc. project so far. He is reviewer and editorial board member of IJEIT. He has been a member of IEEE since 2012, a member of Computer Society of India (CSI) since 2012, a life member of the IACSIT since 2012 and IAENG since 2011. His research interest includes network security & cryptography, Cloud Computing, Data Mining and computational intelligence.

Partiksha Nigam has received her Master of computer Application from Kailash Chandra Bansal Technical Academy, Indore(KCBTA) ,Rajiv Gandhi Teachnical University ,Bhopal .She is currently pursuing M.Phil in Computer Science from Govt. Holkar Science Collage (HSC),Indore, Devi Ahilya University, Indore She is presently working as a lecturer in Department of Computer Science, Mata Jijabai Govt. Girls P.G.College, Indore - India. She has published and presents a research paper in National Conference on Emerging Trend in Computing (ETCOMP).Her research interest includes network security & cryptography, Computer Graphics, Programming Languages and computational intelligence.