IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. V (Mar-Apr. 2014), PP 69-74
www.iosrjournals.org

A Novel Approach for Detection of Blackhole Attacks

Ankita V. Rachh[1], Yatin V. Shukla[2], Tejas R. Rohit[3]
[1]*(C.S.E. Department, B.H. Gardi College of Engineering & Technology, India)*
[2]*(C.S.E/I.T. Department, B.H. Gardi College of Engineering & Technology, India)*
[3]*(Computer Department, Darshan Institute of Engineering & Technology, India)*

Abstract : *The MANET (Mobile Adhoc Network) is a wireless distributed network. It is formed by group of autonomous mobile nodes without any infrastructure like access points. Every node of MANET can acts as router as well as host. It has a basic characteristic of dynamic topology, it means nodes can enter and leave network any time. MANET is vulnerable to many security attacks. Black hole attack is most occurred attack in MANET and very hard to detect which is performed on network layer. Black hole attacks are classified into two types. In single black hole attack, one malicious node will change the route of source to destination and wrong path of malicious node will follow. In collaborative black hole attack one malicious node records packet at one end and send to another malicious node at other end. Black hole attacks are active attacks. In this paper, we propose a solution for detecting black hole attack. Our protocol's name is EBAODV (Enhance Black hole AODV). In this approach, leader nodes are used for detecting black hole nodes.***

Keywords: *AODV, Black hole attack, EBAODV, MANET*

I. INTRODUCTION

The introduction MANET is self organized distributed wireless network. Each node of network is Adhoc, without any infrastructure. In MANET, all wireless nodes can communicate with each other directly. In infrastructure based network all nodes can communicate with access points only. Fig. 1 shows infrastructure network. In MANET each and every node can change their position frequently, so track issues of MANET is good research. Fig. 2 shows Mobile Adhoc network. The basic requirement of MANET is source and destination must be within source's transmission range. If destination is outside the source's range then intermediate nodes behave as routers.

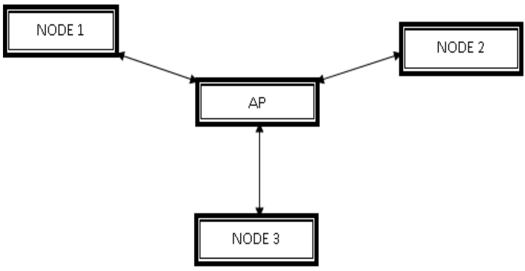


Fig. 1 Infrastructure Network

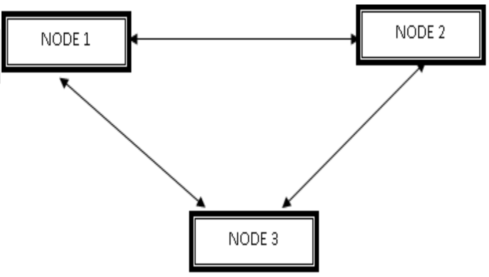


Fig. 2 Mobile Adhoc Network

In MANET, due to dynamic topology link break between routes is occurred. When there is a link break in route, then local route repair occurs [5].

In this paper, we first give introduction of routing protocols in section II. Section III gives information of AODV protocol. In section IV we focus on black hole attack and comparative study of their solutions. Next section focuses on our proposed approach.

II. ROUTING PROTOCOLS

The main goal of routing protocol is to set up an optimal route from source to destination having higher packet delivery and minimum delay [18]. There are three basic types of routing protocols.

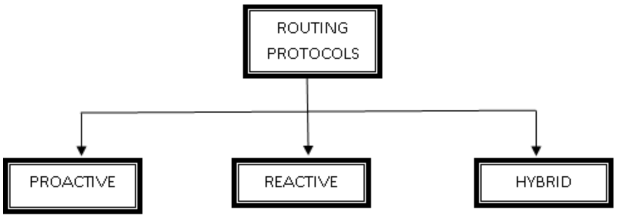


Fig. 3 Routing Protocols

1.1Proactive Routing Protocol

The proactive protocol is table driven protocol as every node maintains route table. Mobile nodes broadcast their routing information to its neighbors. The advantage of proactive routing protocol is network status can be immediately reflected if the malicious attacker joins. The disadvantage is overhead rises as network size increases [9].DSDV (destination sequence distance vector) and OLSR (optimized link state routing) are proactive protocols.

1.2Reactive Routing Protocol

The reactive routing protocol is on demand routing protocol as it transmits data packets when needed. The advantage of reactive protocol is wasted bandwidth induced from cyclically broadcast. The disadvantage is passive routing method leads to some packet loss [9]. DSR (dynamic source routing) and AODV (Adhoc on demand distance vector) are reactive protocols.

1.3Hybrid Routing Protocol

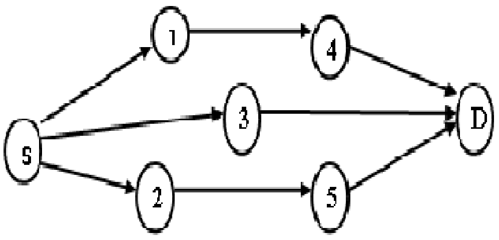
Hybrid routing protocols combines proactive and reactive protocol. ZRP (Zone routing protocol) is best example of hybrid protocol. In ZRP, whole network is divided in various zones. Intra zone routing protocol is proactive and inter zone routing protocol is reactive [1].

III. AODV PROTOCOL

AODV (Adhoc on demand distance vector) protocol is reactive protocol, so route is established when it is required. AODV performs in two steps.

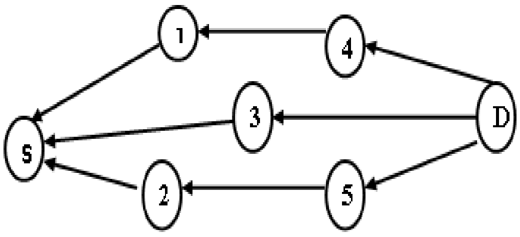
3.1 *Route Discovery*

Route discovery is a process of finding route from source to destination. There are three control messages used for establish routing path. Route Request (RREQ), Route Reply (RREP) and Route Error (RERR).



→ Represents RREQ

Fig. 4 Route Discovery



← Represents RREP

Fig. 5 Reverse Path Setup

Route discovery broadcasts RREQ message into network. A node receives RREQ will check its routing table to see whether it has a path to requested destination [10]. RREP message is used to reply the request message. Source node receives multiple RREP messages and it will select short and fresh path. If there is no route to destination, RREQ is forwarded and it keeps reverse path to source node [10].

AODV uses sequence number to find fresh route. A node which receives RREQ will send RREP if it is either destination or if it has a route to destination with higher sequence number [14]. If any node receives RREQ which have already processed then it is discarded. Shorter and fresher route is selected from source to destination and then actual data packet transmission is started. After sometime, source receives RREP having same or higher sequence number with small hop count. It will update routing and now this will select as best route.

3.2Route Maintenance

Route maintenance commences when any link breaks in source to destination route. Source node will receive route error (RERR) message then it starts route discovery again for finding new route. A routing table entry expires if not used recently [2]. Another way to repair route is local route repair. Repairing node broadcasts RREQ and waits for RREP message. If repairing node fails in receiving RREP it broadcasts RERR to inform other nodes that link is broken.

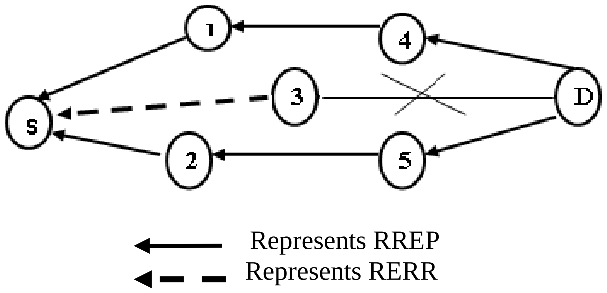


Fig. 6 Route Maintenance

IV. BLACK HOLE ATTACK

Black hole attack is denial of service (DOS) attack. It can be classified into two types. Single black hole attack and Collaborative black hole attack. Occurrence of single black hole attack in MANET is very common and very hard to detect. In single black hole attack one malicious node is there. It claims itself that its path is shortest to destination. This node drops routing packets instead of forward packet to destination [9]. In collaborative black hole attack minimum two malicious nodes are there and transfers packet from one malicious node to another. The aim of black hole attacker is to attract traffic towards it and block data packets by dropping them [16].

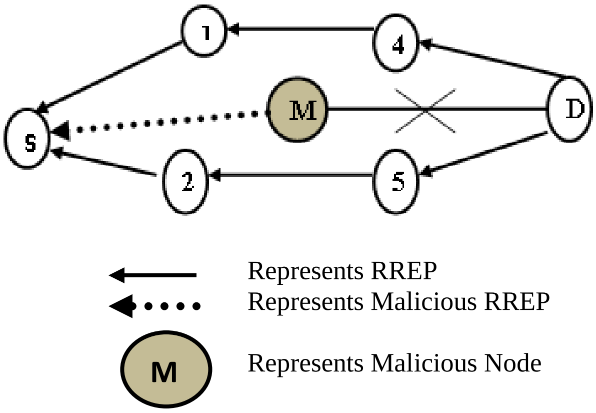


Fig. 7 Black hole attack

In Fig. 7 source node S starts route discovery by sending RREQ message. Malicious node M also receives RREQ message, it sends false RREP message having higher sequence number. Source node S select route from malicious node M. Node M drops packets instead of forwarding and packet delivery ratio of protocol degrades.

In collaborative black hole attack malicious nodes are collaborate together and suspect the route. At least two malicious nodes are required for collaborative black hole attack. It is also known as cooperative black hole attack. Two malicious nodes establish direct wireless link. First malicious node establishes data transmission route and second malicious node drops transmitted data packets [11]. In case of TCP packets, source will come to know about malicious node because it will not receive ACK. In case of UDP packets, source will never come to know about malicious node as UDP do not send ACK [21].Table I summarizes comparative analysis of black hole detection methods.

TABLE I. COMPARATIVE ANALYSIS OF BLACK HOLE DETECTION METHODS

Research Paper	Approach	Performance Matrices	Advantages	Disadvantages
Malicious AODV- Implementations and analysis of routing attacks in MANET[31]	Malicious AODV	Packet efficiency, Throughput, Routing Overhead	Network is partitioned into two parts so attacker cannot degrade performance.	No proper IDS for free environment.
Black hole effect mitigation method in AODV routing protocol [15]	Enhance AODV	PDR using AODV,ERDA and EAODV	Extra route reply message is used from destination and gives better performance.	Throughput and delay's results are not specified.
Securing Routing table update in AODV routing	ERDA	PDR, NRL ratio and delay	Improves process of updating routing entry.	Does not work with outlier detection

[27]				algorithm.
Secure routing protocol to prevent cooperative black hole attack in MANET.[9]	CBD-AODV	PDR and end to end delay	Up to 2.6 times more performance in PDR compare to AODV.	Always wait for second path.
Secure AODV protocol to mitigate black hole attack in MANET.[11]	OAODV(weight updation and feedback method)	PDR with number of node varies and speed of nodes	Improves PDR	False positive
Prevention of selective black hole on MANET[20]	Anti black hole mechanism	Total packet loss	False positive rate is 0%.	For better performance more IDS required.
Improving AODV protocol against black hole attacks[39]	Nital Mistry et. Al's method	PDR and end to end delay	PDR is improved and RREP having high sequence no. is discarded.	More routing overhead.
Prevention of black hole attack in MANET[13]	SAODV	PDR, delay and overhead	No repeated nodes then random path selected and Less overhead.	Increases average end to end delay
A dynamic learning system against black hole attack in AODV[12]	DPRAODV	PDR	Very high PDR	More routing overhead and average end to end delay
Preventing cooperative black hole attack in MANET: Simulation, Implementation and evaluation.[26]	DRI and cross check using FREQ and FREP	Throughput	Very high throughput	More routing overhead

V. PROPOSED WORK

In our proposed solution EBAODV, leader nodes are created first. Leader nodes are used for detection of malicious nodes. From source node RREQ is generated. At that time one timer is used for measuring current time. We can assume any expired time (here 20ms). If RREP received before expired time then one fake packet will send to the destination, this packet is not original data packet. After that if acknowledgement (ACK) receives then original packet will send by source node. If ACK not receives it means packets are dropped. If no. of dropped packets are more than threshold value (here 10) then leader nodes will send block message to all its neighbors. Block message contains id of malicious node. All intermediate nodes receives table having black hole node. Now, again new RREQ message is generated for route discovery.

5.1Flowchart of EBAODV

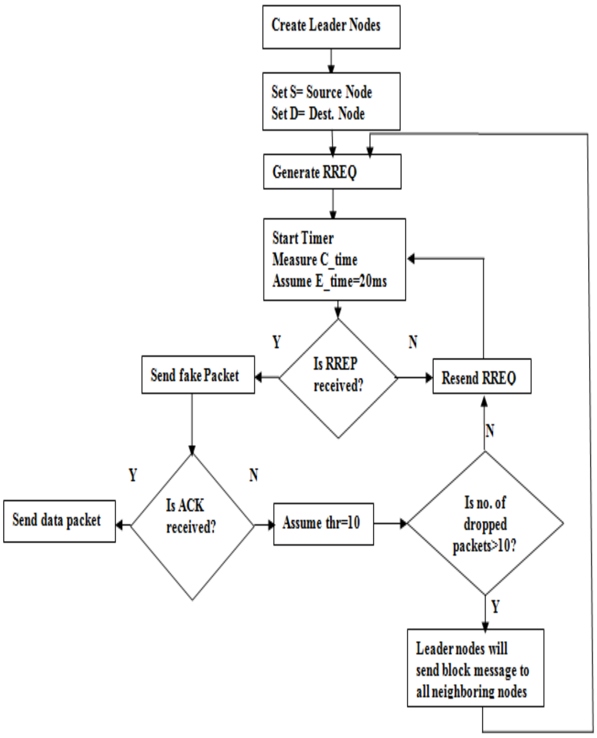


Fig. 8 Flowchart of EBAODV

VI. Conclusions And Future Work

Security is the important issue of routing protocols of MANET. Many attacks are vulnerable to AODV routing protocol of MANET. In AODV routing protocol, nodes having highest sequence number is selected for fresh and short route. In black hole attack malicious node will accept RREQ from source node and drop the packet instead of sending to the destination. In this paper, comparative analysis of black hole detection techniques are also discussed. We propose a new approach EBAODV (Enhance Black hole AODV) which uses leader nodes for detection of black hole. In our approach PDR (packet delivery ratio) and throughput will increase than original AODV.

As part of our future work, we will implement our approach in NS 2 and we will measure PDR, throughput and end to end delay using different parameters.

REFERENCES

[1] Sunil J. Soni , Suketu D. Nayak, "Enhancing Security Features & Performance of AODV Protocol under Attack for MANET", IEEE International Conference on Intelligent Systems and Signal Processing (ISSP),pp-325-328,2013

[2] Sisily Sibichen1, Sreela Sreedhar, "An Efficient AODV Protocol and Encryption Mechanism for Security Issues in Adhoc Networks ", IEEE- ICMICR-2013

[3] Ali M. Sagheer, IEEE Member, and Hadeel M. Taher, "Identity Based Cryptography for Secure AODV Routing Protocol", IEEE-TELFOR,pp-198-201, 2012

[4] Rajesh Yerneni, Anil K. Sarje, "Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc Networks", IEEE-ICCCNT-2012

[5] Christian Gottron, Pedro Larbig, Andr´e K¨onig, Matthias Hollick and Ralf Steinmetz, "The Rise and Fall of the AODV Protocol:A TestBed Study on Practical Routing Attacks", IEEE-LCN-2010

[6] F. Maan, Y. Abbas, N. Mazharg, "Vulnerability Assessment of AODV and SAODV Routing Protocols Against Network Routing Attacks and Performance Comparisons ", IEEE,pp-36-41, 2011

[7] Zaid Ahmad, Kamarularifin Abd. Jalil, Jamalul-lail Ab Manan, "Black hole Effect Mitigation Method in AODV Routing Protocol", IEEE.pp-151-155, 2011

[8] Fidel Thachil, K C Shet, "A trust based approach for AODV protocol to mitigate black hole attack in MANET", IEEE-CPS.pp-281-285, 2012

[9] Nai-Wei Lo and Fang-Ling Liu, "A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET", Springer.pp-59-65, 2013

[10] Junguo Liao and Junwen Li, "ISPM: An Improved Secure Payment Mechanism to Prevent the Black Hole Attack and Selfish Node in WMN", Springer.pp-169-178, 2013

[11] Jayashree Padmanabhan, Tamil Selvan Raman Subramaniam, Kumaresh Prakasam and Vigneswaran Ponpandiyan, "A Secure Routing Protocol to Combat Byzantine and Black Hole Attacks for MANETs", Springer.pp-541-548, 2011

[12] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Springer.pp-1-16, 2011

[13] Davide Cerri and Alessandro Ghioni, "Securing AODV: The A-SAODV Secure Routing Prototype", IEEE.pp-120-125, 2008

[14] Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour, IEEE, "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks", IEEE.pp-2471-2481,May 2009

[15] Kamarularifin Abd. Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan "Mitigation of Black Hole Attacks for AODV Routing Protocol ", IEEE.pp-336-343, 2011

[16] Chanchal Aghi1, Chander Diwaker ," Black hole attack in AODV routing protocol: A Review", IJARCSSE.pp-820-823,April 2013

[17] Alok Rao, Narendra Upadhyay, Vivek Kumar Rai, " A Survey on AODV Protocol Performance with Black Hole Node in MANET" ,IJEAT.pp-574-577, April 2013

[18] Anu Bala, Munish Bansal, Jagpreet Singh, "Performance Analysis of MANET under Blackhole Attack" ,IEEE.pp-141-145, 2009

[19] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks " ,IEEE.pp-556-560, 2012

[20] Ming-Yang Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems" , Elsevier.pp-107-117, 2010

[21] Jan von Mulert ,IanWelch n, Winston K.G.Seah , "Security threats and solutions in MANETs: A case study using AODV and SAODV" , Elsevier.pp-1249-1259, 2012

[22] Debdutta Barman Roy and Rituparna Chaki , "MADSN: Mobile Agent Based Detection of Selfish Node in MANET" ,IJWMN.pp-225-235, August 2011

[23] Radhika Saini and Manju Khari, " An Algorithm to Detect Attacks in Mobile Ad Hoc Network" ,Springer.pp-336-341, 2011

[24] N. Bhalaji1, Alok V. Kanakeri, Krishna P. Chaitanya and A. Shanmugam, "Trust Based Strategy to Resist Collaborative Blackhole Attack in Manet" , Springer.pp-468-474,2010

[25] Nai-Wei Lo and Fang-Ling Liu, "A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET", Springer.pp-59-64, 2013

[26] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "DoS Attacks in Mobile Ad-hoc Networks: A Survey" ,IEEE,pp-535-541, 2012

[27] Kamarularifin Abd Jalil , " Securing Routing Table Update in AODV Routing Protocol" ,IEEE,pp-116-121, September 2011

[28] Hua Qu, Peng Zhang, Ji-hong Zhao, "A New Local Repair Scheme Based on Link Breaks for Mobile Ad Hoc Networks" ,IEEE, pp-364-371, 2009

[29] Jayashree Padmanabhan, Tamil Selvan Raman Subramaniam, Kumaresh Prakasam,and Vigneswaran Ponpandiyan "A Secure Routing Protocol to Combat Byzantine and Black Hole Attacks for MANETs" ,IEEE, pp-541-548,2011

[30] Gunhee Lee · Wonil Kim · Kangseok Kim · Sangyoon Oh · Dong-kyoo Kim ,"An approach to mitigate DoS attack based on routing misbehavior in wireless ad hoc networks ,Springer, May 2013

[31] Humaira Ehsan1, Farrukh Aslam Khan, "Malicious AODV", IEEE,pp-1181-1186, 2012

[32] J. J. Garcia-Luna-Aceves, Fellow, IEEE, ACM, and Rolando Menchaca-Mendez, "PRIME: An Interest-Driven Approach to Integrated Unicast and Multicast Routing in MANETs", IEEE/ACM.pp-1573-1586, December 2011

[33] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, “A Survey of Secure Mobile Ad Hoc Routing Protocols” ,IEEE.pp-78-85, 2008

[34] Charles E. Perkins ,Elizabeth M. Royer, Samir R. Das and Mahesh K. Marina, “Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks”, IEEE.pp-16-28, 2001

[35] Mrs. P.VIGNESWARI, “Comparative Analysis of AODV and Trusted AODV (TAODV) in MANET” ,IJAIST,pp-49-56 ,February 2013

[36] Zehua Wang, Student Member, IEEE, Yuanzhu Chen, “CORMAN: A Novel Cooperative Opportunistic Routing Scheme in Mobile Ad Hoc Networks” ,IEEE.pp-289-296 ,February 2012

[37] Debdutta Barman Roy1 and Rituparna Chaki, “Detection of Denial of Service Attack Due to Selfish Node in MANET by Mobile Agent”, IEEE.pp-14-23, 2011

[38] Shelly Salim and Sangman Mohe, “On-demand routing protocols for cognitive radio ad hoc networks”, Springer, pp-1-10, 2013

[39] Nital Mistry, Devesh C Jinwala, Member, IAENG, Mukesh Zaveri, “Improving AODV Protocol against Blackhole Attacks”, IEEE, March 2010