Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.538 – 543

RESEARCH ARTICLE

Qualitative Analysis of Hybrid Routing Protocols Against Network Layer Attacks in MANET

Apoorva Chandra[1], Sanjeev Thakur[2]

[1]Department of Computer Science and Engineering, Amity University, India

[2]Department of Computer Science and Engineering, Amity University, India

[1] apoorv_11chandra@yahoo.com.sg; [2] sthakur3@amity.edu

Abstract*—This paper gives utmost predictive comparative analysis of two hybrid routing protocol which includes Zone routing protocol (ZRP), Hybrid wireless mesh protocol (HWMP) and reactive protocol which is Adhoc On Demand Distance Vector (AODV) routing protocol against the real time vulnerable security attacks in the network layer. The primary objective is to provide analysis which describes the use of specific hybrid protocol in Mobile adhoc network (MANET) which exhibit secure and efficient packet transmission. The protocols are analysed among different parameters on which there efficiency is evaluated. This paper provides insight to the potential threats which they posses in open communication channel in real time and their effects on the performance. Few parameters are simulated to evaluate the efficiency for protocols. Network layer attacks used in this work for evaluation narrows the possibilities of using inefficient protocols which also concludes the necessity of using specific hybrid routing protocol.

***Keywords*— HWMP, MANET, AODV, Threats, ZRP, Network layer.**

I. INTRODUCTION

During past decade communication channel has been revolutionised from personal computing to handheld computing devices. Subscribers can use wireless communication channel now more easily from anywhere. The channels are open in which users can hop from one network to other frequently changing the network topology due to which devices are prone to security threats which decreases the efficiency of routing protocols. Many researches have been carried on for providing efficient communication medium for packets transmission. Due to open communication channel in MANET the network topology changes dynamically with every new node which connects in the network. Every new node has ability to route packets without letting other nodes to know if they are malicious or authentic node. Attacks which are active or passive could be induced to extract sensitive information during packet routing. Attacks like black hole, gray hole, jellyfish prone more threat to MANET. MANET enables cost effective way of information exchange in day to day use, in military as well as in corporate sector [1]. Traditional routing protocols like proactive and reactive which included Adhoc on Demand Distance Vector routing (AODV) , optimized link state routing (OLSR), Temporally ordered routing algorithm (TORA) etc protocols were created and numerous protocols were improvised for retrieving efficient performance and providing security. But the protocols generating large amount of delay, overhead and failure in route discovery and route maintenance due to lack of security. Further through evolution of protocols from connectionless network topology hybrid routing protocols were build which is the second category of adhoc routing protocols. The performance MANET depends upon the efficiency of the protocol which is being used for packet transmission. Efficiency of protocol depends upon several factor like throughput, end to end delay, security mechanism, bandwidth utilized, communication overhead for routing [2]. The traditional protocols failed to achieve the efficiency and security needed for secure transmission of packets.

Through collaboration of on demand routing i.e. reactive routing and table driven i.e. proactive routing hybrid routing protocols are made. They provide better performance and secure packet transmission [3]. Hybrid routing protocols include Zone Routing Protocol (ZRP), Zone based hierarchical link state routing (ZHLS) protocol, Hybrid wireless mesh protocol (HWMP). Proactive and reactive routing protocol like AODV create large amount of end to end delay during route discovery and maintaining routing table which were overcome in hybrid protocols. But for enhanced performance and efficiency ZRP is used, due to its route maintenance and route discovery technique. Zone based hierarchical link state (ZHLS) routing and Hybrid wireless mesh protocol (HWMP) which show similar features as ZRP are not used, reasons will be further discussed in this paper. There has been no concluding research which indicates the reason of not using any other hybrid techniques over ZRP. Although ZHLS and HWMP provide more accuracy than ZRP still they have not been used which leads to primary objective of this paper.

II. ROUTING PROTOCOLS

Hybrid routing protocols comprises all essential features of both flat routing protocols which are reactive and proactive routing protocols and while inheriting there essential functionalities mitigates the setbacks of both routing protocols. Reactive and proactive techniques are proven to be best in their individual topology but due to change in topology due to mobile devices in wireless network hybrid routing is used to make balance using both techniques in hybrid routing. In this proactive technique provides efficient route discovery and route maintenance from source node to destination within small region where as reactive technique is used for route discover and maintenance outside the zone [4].

A. *Types of Hybrid routing protocols*

1) *Zone routing protocol (ZRP):* ZRP is created by two protocols Intrazone Routing Protocol (IARP) and Interzone Routing protocol (IERP). IARP works as the proactive part in the routing which enhances the reactive part of the protocol. The functionality of IARP solely depends upon neighbour discover protocol (NDP) to provide nodes which are near for packet transmission. It also uses the TTL (Time to Live) constraint which is used during the packet transmission when the node routes from one node or router the value of TTL decreases by one and as soon as the value becomes zero packets stops rebroadcasting [5].
   IERP works as the reactive part of ZRP protocol which is used for route discovery outside the zone area for packet transmission. This mechanism is not called till the packet seeking destinations is outside the zone. It initiates route discovery rather than sending packets neighbour to neighbour till it reaches the destination [6].

2) *Hybrid Wireless Mesh Protocol (HWMP):* For IEEE 802.11s networks HWMP is used which comprises both reactive and proactive techniques. For packet transmission in this four messages are used which are: path request (PREQ), path reply (PREP), path error (PERR) and root announcement (RANN). For discarding older path HWMP uses destination sequence number. New routes have small sequence number as compared to older path which enables discarding older path and avoids loops in routing also called as “counting to infinity”. In the reactive part of HWMP when the packets are needed to be routed the source sends RREQ messages containing destination point and zero are initialized to metric. When source receives smaller sequence number then RREQ then metric is updated. When the path is traversed for finding path and search is complete then destination node sends RREP unicast messages to intermediate nodes and which sends back to source node [7].

   Now, the proactive part has again two mechanism proactive route request and proactive RANN. In proactive RREQ which create tree process provided by root node. It has metric set to 0 by root node and sequence number. Each node receives proactive RREQ which in turn tends to update the metrics. If PREQ contains proactive PREP within itself, then bit is set to 0. Node sends PREP which sets path from root to destination node and if the root changes bit set is set to 1. Proactive RANN sends RANN message in the network regularly. When the RANN messages are received each node trying to get new path sends unicast RREQ to root through root node. Root node then feedbacks with PREP which creates forward path from node to root node. When path changes then PREP is send to the root using new node.

   HWMP is mesh protocol but due to its nature of hybrid it is categorized into hybrid routing protocol.

3) *Adhoc On demand Distance Vector (AODV) routing protocol*: In this protocol the routes are kept for packet transmission as long as they are needed by the source node. It has three control messages route request (RREQ) message, route reply (RREP) and route error (RERR) message. RREQ messages are sent when the source nodes needs the route for packets transmission. RREQ has time to live (TTL) value which counts the number of hops for transmission which increases at retransmission. RREP messages are send in unicast to source node when valid path is available. Every node scrutinizes the next hop. RERR error is sent to notify all nodes when the link break occurs in active communication route [8].

B) *Types of attacks*

The analysis is carried out based on following attacks:

1) *Black Hole Attack:* In this attacks attacker nodes sends path reply message to path request message containing minimum sequence number for routing and before any valid reply comes from any authentic node source node assumes the attacker node is the valid route and starts packet transmission over false nodes. The packets forwarded through this attacker node are never forwarded to any other node. This type of attack takes place when attacker node is inside the network and attacker continuously asks for packet which leads to sleep deprived attack of the node [9]. It can be considered as denial of service attack as it receives all packets and send none. It is named black hole as all packets forwarded to it are never forwarded to any other nodes which leads to denial of service.
   There are two types of black hole attack: Single black hole attack in which single node behaves as the black hole node in the network. Second one is collaborative black hole attack in which multiple black hole nodes are inside single network.

2) *Gray Hole attack:* Gray hole attack occurs when the attacker nodes only keep the packets which are required by the attacker and rest all nodes are dropped. It is also called routing misbehavior, as in this the attacker node accepts the node to forward but once received they are dropped selectively [10]. This type of attack also leads to denial of service attack.

3) *Jelly fish re-ordering (JFR) attack:* In this attack the attacker knows the vulnerability in Transmission Control Protocol (TCP) uses it to re order packets. It occurs due to route changes or because of multi path routing. It is passive attack and so it’s hard to detect [11]. JFR also increases the end to end delay of the packets in some cases.

III. COMPARISON AND ANALYSIS

Analysis has been disseminated into two parts quantitative and qualitative. Quantitative parameters have been simulated into the NS2 simulator and qualitative parameters have been concluded on the basis of analytical research. The throughput and the average end to end delay has been compared among the basic protocol simulation, with black hole attack, with gray hole attack and with jelly fish reorder. All three protocols were simulated into same network scenario for throughput and average end to end delay.

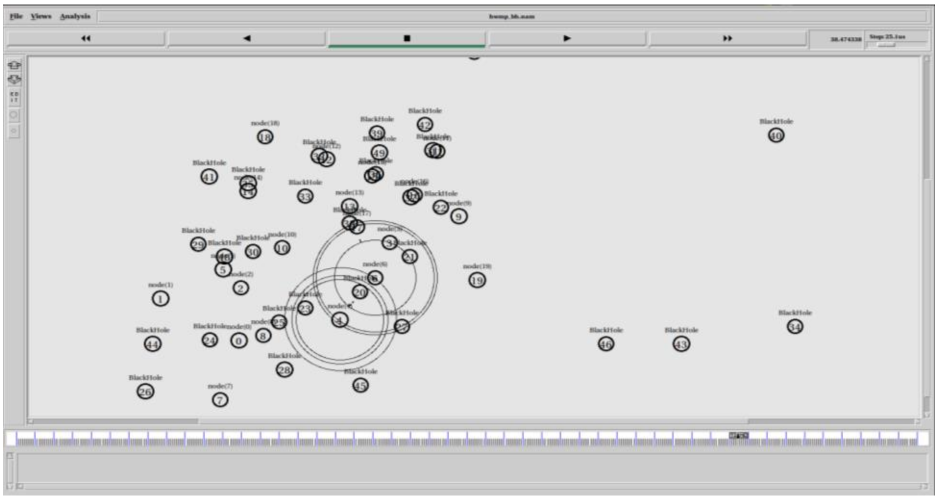

Fig 1 Simulation of HWMP protocol with black hole attack

Fig 1 shows simulation of HWMP with black hole attack . Similar simulation has been carried for ZRP and AODV for 50 nodes for each scenario.

A) *Analysis of the hybrid protocols and reactive protocol:*

Parameters used for analysis:

1. *Throughput (Simulated in NS 2 simulator):* Throughput is the rate at which the packets are transmitted per second, in this case 1024 bits per second.
2. *Average end to end delay (Simulated in NS 2 simulator):* It is the time needed by the packet to reach from source to destination.
3. *Classification:* It's the category in which protocols has been designed.
4. *Metrics for path finding:* It is the path find algorithms used.
5. *Route discovery:* Protocols needed for route discovery.
6. *Applicable network attacks:* Network layer attacks which could disrupt the proper functioning of the network.
7. *OSI layer:* Open System Interconnection layer at which the protocols works.

B) *Quantitative Comparison of ZRP, HWMP, AODV against black hole , gray hole and Jellyfish reorder attacks:*

The hybrid routing protocols have been simulated in network simulator NS 2 for quantitative parameters for analysis remaining all are qualitative parameters concluded through study.

TABLE 1
QUANTITAIVE ANALYSIS OF ZRP AGAINST NETWORK ATTACKS

S.No	**Parameters**	**ZRP**	**ZRP_BH**	**ZRP_GH**	**ZRP_JFR**
1.	Throughput [In KBPS]	117.16	103.3	103.3	117.16
2.	Average end to end delay	150.2	152.13	152.31	150.2

BH - black hole attack (in all Tables)
GH – Gray hole attack (in all Tables)
JFR – Jelly fish reorder attack (in all Tables)

It is seen in Table 1 that the protocol the throughput for the normal ZRP is same as the throughput with JFR which is the jelly fish reorder attack. The throughput performance at black hole and gray hole are same. So it is shown that black hole attack and gray hole attack produce same throughput and normal and JFR produce the same throughput. Similarly gray hole and black hole remains the same and average E to E delay was same for gray hole and black hole.

TABLE 2
QUANTITAIVE ANALYSIS OF HWMP AGAINST NETWORK ATTACKS

S.No.	**Parameters**	**HWMP**	**HWMP_BH**	**HWMP_GH**	**HWMP_JFR**
1.	Throughput [In KBPS]	170.04	135.35	135.35	159.19
2.	Average end to end delay	134.38	105.38	105.38	129.16

In Table 2 it was evaluated that the attacks which were made on ZRP proved to be more disrupting in HWMP implementation. The throughput of HWMP with JFR is 159.19 and without JFR its 170.04 kbps which indicated that JFR is capable to attack HWMP protocols as well as the average end to end delay decreases which shows vulnerability in HWMP against JFR..

TABLE 3
QUANTITAIVE ANALYSIS OF AODVAGAINST NETWORK ATTACKS

S.No.	**Parameters**	**AODV**	**AODV_BH**	**AODV_GH**	**AODV_JFR**
1.	Throughput [In KBPS]	164.35	162.97	219.79	165.16
2.	Average end to end delay	143.96	139.39	147.05	142.55

As AODV is one of the earliest routing protocol it was also evaluated against network attacks to see whether the HWMP or AODV exhibits more efficiency than ZRP but it was seen that the throughput, average end to end delay is far less than ZRP and HWMP. Although it is shown in table that throughput of AODV is greater than ZRP and HWMP but actually when the node size increased from 50 to multiples 100 which is 200 to 300 the overhead increased and the throughput also decreased.

C) Qualitative comparison of protocols:

TABLE 4
QUALITATIVE ANALYSIS OF PROTOCOLS

S.No.	**Parameters**	**ZRP**	**HWMP**	**AODV**
1.	**Classification**	Hybrid	Hybrid	Reactive
2.	**Metrics**	Shortest path	Distance vector/tree based	Distance vector
3.	**Route Discovery**	Interzone & Intrazone	Reactive route discovery &Proactive routing	On demand
4.	**Network attacks**	None	Jelly fish reorder	Black hole
5.	**OSI layer**	Network layer	Data Link layer	Network layer
6.	**Throughput ***	Low	Medium	High
8.	**Avg End To End Delay***	Low	High	Medium

* - Throughput against network layer attacks
* - Average end to end delay is deduced from table 1, 2 and 3.

IV. CONCLUSION

The phase shift in use of handheld devices from personal computing has been pushing the technology to its limits. The routing protocols used in packet delivery on real time network need to be secure and efficient in every scenario. This paper concludes that the ZRP routing protocol still is the efficient and most secure packet transmission protocol. The Simulation concluded the parametric evaluation of throughput and end to end delay while the qualitative analysis proved the basic structural and behavioural difference in these three protocols. The hybrid routing protocols still will be preferred over any other routing protocols for reliable packet transmission.

V. FUTURE SCOPE

This work explores new possibility of enhancing HWMP as it can be used as the substitute of ZRP in near future. New protocols could be tested against other protocols similar to this work , still few protocols are not tested which strives to explore the possibility in generation of more reliable packet transmission protocol.

References

[1] K .Lego, P. K. Singh, D. Sutradhar, *"*Comparative Study of Adhoc Routing Protocol AODV, DSR and DSDV in Mobile Adhoc NETwork*", Indian Journal of Computer Science and Engineering*, Vol. 1 No. 4 364-371, 2011.

[2] G. Lakshmikant, A Gaiwak, P.D. Vyavahare, *"*Simulation Based Comparative Performance Analysis of Adhoc Routing Protocols*", in proceedings of TENCON 2008*.

[3] A. K. Gupta, H. Sadawarti, and A. K. Verma , "Review of Various Routing Protocols for MANETs", *International Journal of Information and Electronics Engineering,* Vol. 1, No. 3, pp. 251-259, November 2011

[4] Z. J. Haas, M. R. Pearlman, and P. Samar, "The Intrazone Routing Protocol (IARP) for Ad Hoc Networks," Internet Engineering Task Force (IETF) draft, draft-ietf-manet-zone-iarp-02.txt., July 2002.

[5] Z. J. Haas, M. R. Pearlman, and P. Samar, "The Interzone Routing Protocol (IERP) for Ad Hoc Networks," Internet Engineering Task Force (IETF) draft, July 2002. Draft-ietf-manet-zone-ierp-02.txt.

[6] Jian-feng Ma, Zi-hui Miao, Kai Yang, "Hybrid Routing Protocol for Wireless Mesh Network", *International Conference on Computational Intelligence and Security*, Beijing, Vol. 1, pp. 547 - 551 , November 2009

[7] A. Hadi, A. Rahman and Z.A. Zukarnain,, "Performance Comparison of AODV, DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc Networks‖", *European Journal of Scientific Research*, Vol.31 No.4, pp.566-576, 2009.

[8] Harjeet Kaur , Manju Bala, Varsha Sahni , "Study of Black-hole Attack Using Different routing Protocols in Manet" , *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, Vol. 2, Issue 7, pp. 3031-3038, 2013

[9] K. Gupta, M. Gujral , Nidhi, "Secure Detection Technique Against Blackhole Attack For Zone Routing Protocol in MANETS", *International Journal of Application or Innovation in Engineering & Management*, Vol 2, Issue 6, June 2013

[10] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar , "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", *International Conference on Information, Communications & Signal Processing,* , pp. 1-5 , Singapore ,December 2007

[11] Hepikumar R. Khirasariya, "Simulation study of Jellyfish in MANER (mobile ad hoc network) using AODV routing protocol", *Journal of Information , knowledge and research in computer engineering*, , Volume 02, issue 02, pp. 344-347, 2013.