Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Detection and Prevention of Sinkhole Attack on Zone Routing Protocol (ZRP) in MANET

M.Kayalvizhi[1], Mr.G.Arul Kumaran[2], A.Nithyasri[3]

[1]PG Scholar, Dept .of Information Technology, Vivekananda College of Engineering for Women Tiruchengode – 637205, Tamilnadu, India
[2]Assistant Professor, Dept. of Information Technology, Vivekananda College of Engineering for Women Tiruchengode – 637205, Tamilnadu, India
[3]Assistant Professor, Dept. of Information Technology, Vivekananda College of Engineering for Women, Tiruchengode – 637205, Tamilnadu, India

Abstract—Mobile Ad-hoc Network (MANET) is a kind of wireless network. A Wireless ad-hoc network is a temporary network with no network infrastructure. The nodes communicate with each other, they co-operate by forwarding data packets to other nodes in the network. Thus the nodes find a path to the destination node using routing protocols. Due to the security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Sinkhole Attack. Sinkhole attack is a kind of routing attack in MANET. A sinkhole node tries to attract all the network packets to it-self from all neighboring nodes. This paper focuses on to detect and prevent sinkhole node. By using a hybrid detection technique which combines the advantages of both reactive and proactive routing Protocol to detect the black hole node. It also shows performance of ZRP.

Keyword— *MANET, ZRP, Reactive, Proactive, Sinkhole.*

1. INTRODUCTION

A Mobile Ad hoc Networks (MANET) is a system of wireless mobile nodes that can freely and dynamically self-organize in arbitrary and temporary network topologies without the need of a wired backbone or a centralized administration. People and devices can be seamlessly internetworked in areas without any preexisting communication infrastructure or when the use of such infrastructure requires wireless extension.

Mobile ad hoc networking offers unique benefits and versatility for certain environments and applications. First, since they have no infrastructure including base station as prerequisites, they can be created and used anytime, anywhere. Second , such networks can be intrinsically fault resilient, for they do not operate under the limitations of a fixed topology. Indeed, since all nodes are allowed to be mobile, the composition of such networks is necessarily time varying. Addition and deletion of nodes occurs only by interactions with other nodes; no other is involved.

Such perceived advantages elicited immediate interest in the early days among military, police, and rescue agencies in the use of such networks, especially under disorganized or hostile conditions, including isolated scenes of natural disaster or armed conflict. Soldiers equipped with multimode mobile communicators can now communicate in ad hoc manner without the need for fixed wireless base stations.

A hybrid protocol is a combination of both reactive & proactive routing protocols.ZRP is one of the hybrid protocol and it more efficient, and effective routing protocol. The security issue has become one of the major concerns & challenge in MANET due to its characteristics, especially for those selecting sensitive applications. In most of the routing protocols for MANET, in order to communicate beyond their transmission range nodes takes cooperation to forward packets to each other which exposes them to a wide range of security attacks, which can be classified into two types as passive & active attack.

Sinkhole is one of severe representative attack in MANET under which ZRP needs to be evaluated, where malicious node attempts to draw all network traffic towards it by broadcasting fake routing information & modify or drops packets sent for forwarding which leads to performance degradation of network. The performance of any routing protocol can be realized quantitatively by means of various performance metrics such as packet Delivery ratio, end to end delay, and throughput & packet loss.

The rest of the paper is organized as follows: Section 2 presents Overview of MANET protocol, while section 3 describe Zone Routing Protocol in detail, section 4 describe Sinkhole attack in detail, while section 5 describe proposed work, while section 6 describe result analysis and, while section 7 concludes this paper.

2. MANET 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. There are three basic types of routing protocols.

2.1 Proactive Routing Protocol

The proactive routing protocol is table driven protocol. It attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node maintain one or more tables to store routing information, and they respond to changes in network topology by propagating route updates throughout the network to maintain a consistent network view. The areas where they differ are the number of necessary routing –related tables and the methods by which changes in network structure are broadcast. DSDV (Destination Sequence Distance Vector) and OLSR(Optimized Link State Routing) are proactive protocols.

2.2 Reactive Routing Protocol

The reactive routing protocol is on demand routing protocol. On-demand approach is different from table-driven routing is source-initiated on-demand routing. This type of routing creates routes only when desired by the source node. When a node route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined. Once a route has been discovered and established, it is maintained by some form of route maintenance procedure until either the destination becomes inaccessible along every path from the source or the route is no longer desired.

DSR (dynamic source routing) and AODV (Ad hoc on demand distance vector) are reactive protocols.

2.3 Hybrid 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.

3. ZRP – ZONE ROUTING PROTOCOL

ZRP (Zone Routing Protocol) is a hybrid protocol incorporating the merits of on-demand and proactive routing protocols. A routing zone is similar to a cluster with the exception that every node acts as a cluster head and a member of other cluster. Zones can overlap. Each node specifies a zone radius in terms of radio hops. The size of a chosen zone can, therefore, affect ad hoc communication performance.

In ZRP, a routing zone comprises a few mobile ad hoc nodes within one, two, or more hops away from where the central node is formed. Within this zone, a table-driven-based routing protocol is used. This implies that route updates are performed for nodes within the node. Each node, therefore, has a route to all other nodes within the zone. If the destination node resides outside the source zone, an on-demand search-query routing method is used.

ZRP itself has three sub-protocols: (a) the proactive (table driven) Intra zone Routing Protocol (IARP), (b) the reactive Inter zone Routing Protocol (IERP), (c) the Border cast Resolution Protocol (BRP). IARP can be implemented using existing link-state or distance-vector routing.

ZRP's IARP relies on an underlying neighbor discovery protocol to detect the presence and absence of neighboring nodes, and therefore, link connectivity to these nodes. Its main role is to ensure that each node within the zone has a consistent routing table that is up-to-date and reflects information on how to reach all other nodes in the zone.

IERP, however, relies on border nodes to perform on-demand routing to search for routing information to nodes residing outside its current zone. Instead of allowing the query broadcast to penetrate into nodes within other zones, the border nodes in other zones that receive this message will not propagate it further. IERP uses the border cast resolution protocol.

Because parts of an ad hoc route are running different routing protocols, their characteristics will therefore be different. Some parts of the route is dependent on proper routing convergence, while the other part is dependent on how accurate the discovered inter zone route is. This can make assurance of routing stability very difficult. Without proper query control, ZRP can actually perform worse than standard flooding-based protocols.

ZRP's route discovery process is, therefore, route table lookup and/or inter zone route query search. When a route is broken due to node mobility, if the source of the mobility is within the zone, it will be treated like a link change event and an event-driven route updates used in proactive routing will inform all other nodes in the zone. If the source of mobility is a result of the border node or other zone nodes, then route repair in the form of a route query search is performed, or in the worst case, the source node is informed of route failure.

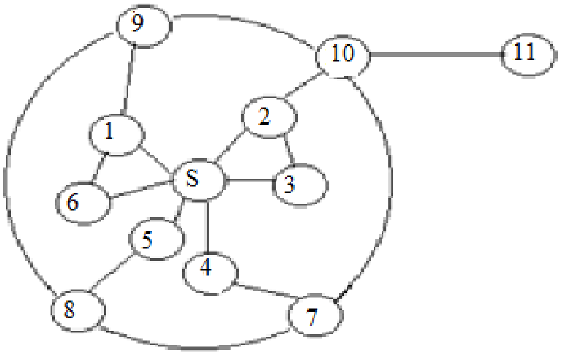

Fig .1 Example routing zone with r=2

The nodes of a zone are partitioned into horizon nodes and interior nodes. Horizon nodes are those nodes whose minimum distance from the centre node is exactly equal to the zone radius **r**. The nodes whose, minimal distance is comparatively less than radius **r** are interior nodes. The nodes having distance equal to zone radius **r** are horizon nodes and nodes with distance more than radius **r** are exterior nodes. In Figure 1, the nodes 1, 2, 3, 4, 5 and 6 are interior nodes; the nodes 7, 8, 9 and 10 are horizon nodes and node 11 lies outside the routing zone. The node 9 can be reached in two ways, one with hop count 2 and another with hop count 3. The node is said to be within the zone, because the shortest path is less than or equal to the zone radius.

We are assuming that:-

- The radius of the zone will be **r** = 2
- The nodes within the zone will be called as neighbor nodes for each other.
- It may be possible that a node belongs to multiple zones. That means overlapping zones are possible.

We are categorizing nodes in four as:

- Interior nodes- nodes that are within the zone (Hop Count <**r**).
- Horizon nodes- nodes that are on the periphery and within the zone (Hop Count = **r**).
- Exterior nodes- nodes that are outside the zone (Hop Count >**r**).
- Bouncer nodes- on the periphery with privilege (Hop Count = **r**) and considered that it can never be compromised.

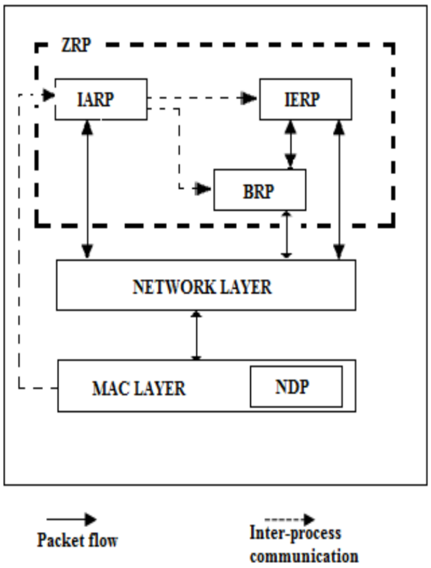

Fig. 2 ZRP architecture

4. ANALYSIS OF SINKHOLE PROBLEM

Sinkhole node tries to attract data to itself by convincing neighbors through broadcasting fake routing information & let them know the specific nodes for their way. By this procedure, sinkhole node attempts to draw all network traffic to itself. Then it alters the data packet or drops the packet silently. It increases network overhead, decreases network's life time by boosting energy consumption. Finally destroy the network.

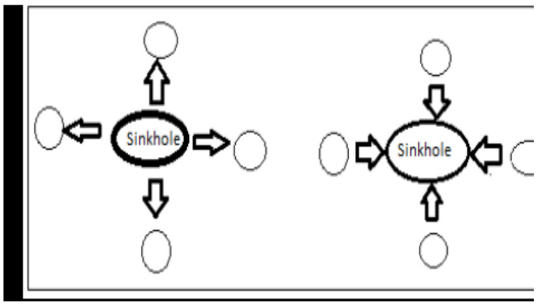

Fig.3 Sinkhole Problem

In ZRP protocol, sinkhole attack is set up by modifying sequence number in RREQ, higher the sequence number, then route will be more recent the packet contains. Sinkhole node selects the source, destination node. It observes the source node's sequence number carefully, and generates bogus RREQ with selected source, destination and higher sequence number than observed source sequence number. It then broadcasts the bogus RREQ. Nodes that take this bogus RREQ recognize that this route could be a better route to the source than incumbent route.

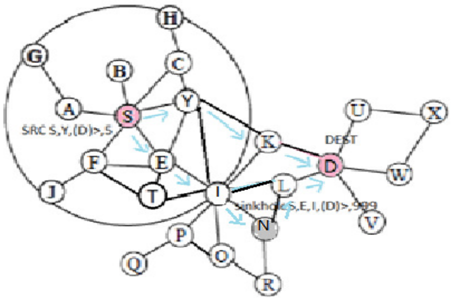

Fig.4 Bogus RREQ Propagation

In Fig.4 shows the propagation of the bogus RREQ packet. Sinkhole node N makes the bogus RREQ. Sequence number of bogus packet is 999, much higher than original source's, 5.

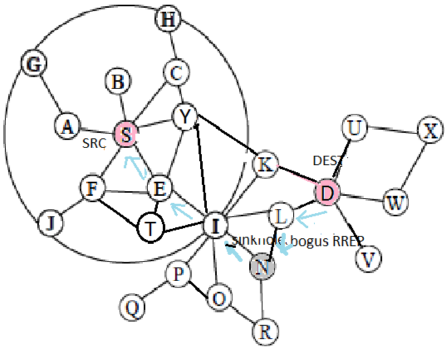

Fig.5 Bogus RREP Propagation

Bogus RREP is shown in the above Fig.5 where destination node thinks that route having sinkhole node is shortest, to reach to source node. Sinkhole node N can easily repeat this procedure & can draw all local network traffic to itself. Then node N can do malicious acts including dropping, or modifying the traffic.

5. PROPOSED WORK

IARP is proactive protocol and is used inside the zone whereas IERP is reactive protocol and is used between the routing zones. Due to the sensibility of IERP, IERP is weaker than IARP.There is no security method in the ZRP. In this paper we are proposing a secure mechanism against sinkhole attack for ZRP protocol viz. Secure Detection Technique (SDT).

In SDT algorithm, we have divided security in two parts:-
(i) When communication takes place within the local zone.
(ii) When inter zone communication takes place.

In this algorithm a code for con probe packet has been written, this code helps in discovering and preventing sinkhole node. When communication takes place within local zone, source node floods the con probe packet. This packet contains an illusionary address of non-existent (NE) node.

This packet is received by the immediate neighbor. All the neighboring nodes check their entries in the routing table than they forward message to their immediate neighbor only if they are not sinkhole node. If there is a sinkhole node present in the zone, then it will rapidly response to the packet it receives from source node through the intermediate node.

After receiving reply from sinkhole node, source node detects it as a malicious node present in the network. After this, the source node sends information to its immediate neighbor for updating their entries and block sinkhole node. Each intermediate node from source to sinkhole node will make an entry for caught sinkhole node. This algorithm works for the security for inter zone communication as well as intra zone communication. Suppose, N1, N2, N3…Nn-1are the nodes between the source N0 and the destination Nn (we are considering Nn as sinkhole node).

5.1 Secure Detection Technique

The SDT for ZRP is based on the following algorithm-

```
Step-1
        1 Source, N0
        2 Generate REQ (NE) IARP
        3 Forward REQ (NE) IERP/BRP
Step-2
        4 Intermediate Nodes N1, N2 …Nn-2
        5 Propagate REQ (NE) IERP/BRP
Step-3
        6 Previous Next Hop Nn-1
        7 Deliver REQ (NE) IERP/BRP
Step-4
        8 Destination (sinkhole node) Nn
        9 REP (NE) IERP/BRP
Step-5
        10 Previous Next Hop Nn-1
        11 REP (NE) Nn-1
Step-6
        12 Source, N0
        13 Receive REP (NE) Nn-1 …N2, N1
        14 Send BLOCK (Nn, NE) IERP/BRP
        15 Update SINKHOLE node Entry
Step-7
        16 Nn-1
        17 Receive BLOCK (Nn, NE) IERP/BRP
        18 Delete Route Entry (NE)
        19 Update Neighboring Node
```

The algorithm works as-

To catch the sinkhole node, source node N0 sends con probe packet i.e. REQ packet which contains the address of the non-existent destination node, to the immediate neighbor node N2. Neighbor node checks its routing table for entry of destination node. If there is no entry in the table it will propagate the REQ message to the intermediate nodes till Nn-1 node. Previous Next Hop Nn-1 delivers this REQ packet to the destination Nn. The destination sinkhole node Nn then quickly send a reply REP packet correspond to REQ packet saying that it has a shortest route for non-existent destination node. The Nn node sends this REP packet back to the nodes in the discovered route. Source node N0receives REP (NE) Nn-1…N2, N1 packet and send BLOCK (Nn, NE) IERP/BRP packet to Nn-1 node. Now the source node broadcast this information to all nodes to block and delete entry for Nn node and also each intermediate node will update sinkhole node entry in separate table.

6. RESULT ANALYSIS

6.1 Packet Delivery Ratio

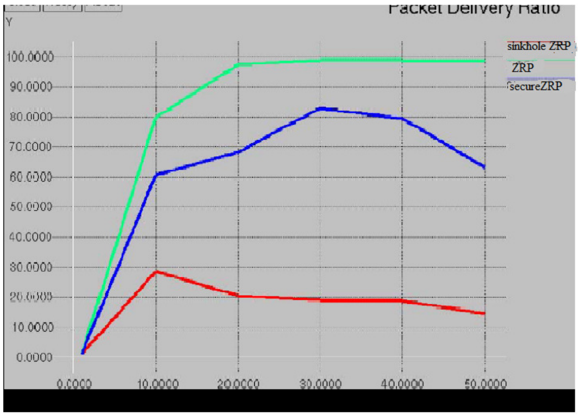

Fig.6 PDR vs. no. of nodes

From above graph we can say that value of PDR is increasing linearly for original ZRP when we vary number of nodes from 10 to 50 as well PDR values for sinkhole ZRP is low. At the same time values of PDR for secure ZRP is improved compare to sinkhole ZRP.

6.2 Packet Loss

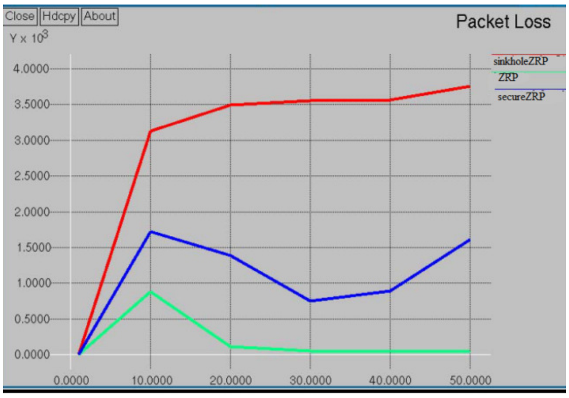

Fig.7 Packet loss vs. no. of nodes

From above graph we can say that, the packet loss for original ZRP decreasing constantly when we vary number of nodes from 10 to 50 at the same time packet loss for sinkhole ZRP is high compare to original ZRP for same variation of nodes & packet loss for secure ZRP is less as compare to sinkhole AODV for same variation of nodes.

6.3 Throughput

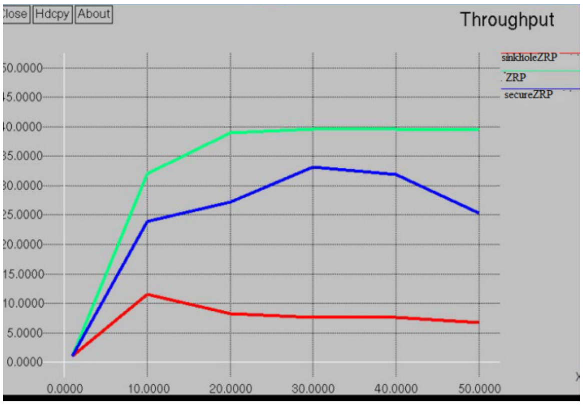

Fig.8 Throughput vs no.of nodes

From above graph we can say that, the throughput for original ZRP is continuously increasing when we vary number of nodes from 10 to 50 at same time its value for sinkhole ZRP is low compare to original ZRP for same variation of nodes but its value for secure ZRP is improved compare to sinkhole.

6.4 End to End Delay

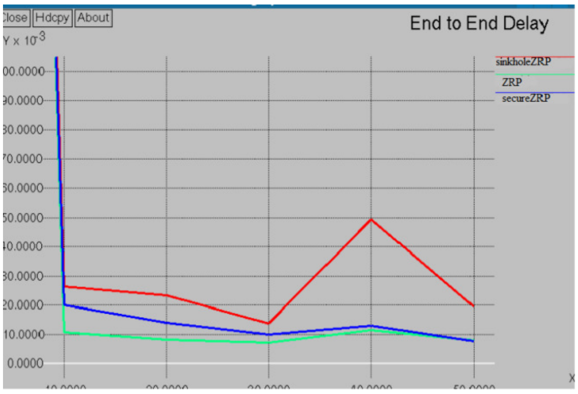

Fig.9 Delay vs. no. of nodes

From above graph we can say that value of end to end delay for original ZRP is decreasing but not constantly when we vary number of nodes from 10 to 50, end to end delay for sinkhole ZRP is high compare to original ZRP, but at same time, end to end delay for secure ZRP is improved compared to sinkhole ZRP.

7. CONCLUSION

This paper has proposed sinkhole attack detection and prevention mechanism by using ZRP. This paper also evaluate the performance of ZRP is improved after applying this mechanism which is deteriorated due to attack. In this paper mainly focus on analyze & study sinkhole problem on the context of other routing protocols and to evaluate variation in its performance after applying for detection and prevention mechanism by considering other performance metric.

REFERENCES

[1] Benjamin J. Culpepper, H.Chris Tseng," Sinkhole Intrusion Indicator in DSMANET", First International Conference on broad and networks IEEE 2004.

[2] Gisung Kim, Younggoo Han, SehunKim, "A cooperative-sinkhole detection method for mobile ad hoc networks", International Journal of Electronics and Communication 64 (2010) 390–397".

[3] Kisung Kim and Sehun Kim," A Sinkhole Detection Method based on Incremental Learning in Wireless Ad Hoc Networks", Korea Advanced Institute of Science & Technology Korea.

[4] Haas, Zygmunt J., Pearlman, Marc R., Samar, P.:Intrazone Routing Protocol (IARP), June 2001,IETF Internet Draft, draft-ietf-manet-iarp-01.txt

[5] Haas, Zygmunt J., Pearlman, Marc R., Samar, P.:Interzone Routing Protocol (IERP), June 2001,IETF Internet Draft, draft-ietf-manet-ierp-01.txt

[6] Haas, Zygmunt J., Pearlman, Marc R., Samar, P.:The Bordercast Resolution Protocol (BRP) for AdHoc Networks, June 2001, IETF Internet Draft,draft-ietf-manet-brp-01.txt

[7] Ashish K. Maurya, Dinesh Singh , " Simulation based Performance Comparison of AODV, FSR and ZRP Routing Protocols in MANET",International Journal of Computer Applications (0975 – 8887) Volume 12– No.2, November 2010

[8] H. C. Tseng, B. J. Culpepper, "Sinkhole intrusion in mobile ad hoc networks: The problem and some detection indicators",

[9] Analysis of the Effect of Sinkhole Attack on AODV Protocol In Mobile Adhoc Network by Nisarg Gandhewar

[10] Review on Sinkhole Detection Techniques in Mobile Adhoc Network by Nisarg ssGandhewar

[11] Subramanya Bhat.M & Shwetha.D," A Performance Study of Proactive, Reactive and Hybrid Routing Protocols using Qualnet Simulator" International Journal of Computer Applications (0975 – 8887) Volume 28– No.5, August 2011.

[12] Thanachais Thumthawatworn†, Tapanan Yeophantong and Punthep Sirikriengkrai," Adaptive Sinkhole Detection on Wireless Ad Hoc Networks", Assumption University, Thailand. IEEE 2006.

[13] Charles E. Perkins and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector Routing," Proceeding of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99), New Orleans, LA, USA, February 1999, pages 90-100.

[14] David B. Johnson, David A. Maltz, and Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks," In Ad Hoc Networking, edited by Charles E. Perkins, chapter 5, pages 139-172, Addison-Wesley, 2001.

[15] David Oliver Jorg, "Performance Comparison of MANET Routing Protocols In Different Network Sizes", Computer Science Project ,Institute of Computer Science and Applied Mathematics, sComputer Networks and Distributed Systems (RVS), University of Berne, Switzerland, 2003.

[16] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Chapter 12 2006 Springer.

[17] Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, volume (2) issue (3).