Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Routing Protocols and Attacks in Mobile Adhoc Networks (MANETs)

[1]Swati Kapoor*, [2]Poonam Saini
[1]Research Scholar, [2]Assistant Professor
Department of Computer Science and Engg.
PEC University of Technology, Chandigarh, India

Abstract— A Mobile Adhoc Network (MANET) is collection of mobile nodes that share a wireless channel with no centralized support. These mobile nodes provide communication among themselves using intermediate nodes. Therefore, infrastructure less, dynamic nature, decentralized support makes Mobile Adhoc networks extremely prone to attacks. Moreover, due to high mobility, the efficient routing of packets is affected. The proactive routing protocols have better packet delivery ratios, while the reactive routing protocols have low overheads. Thus, the design of hybrid routing protocols is preferred which combines the advantages of both proactive and reactive routing. Above all, the goal is to enhance security into the routing of packets from one node to another node. Therefore, security becomes a key factor in the design of routing protocols in MANETs. The paper discusses various attacks in order to analyze their impact on routing protocols and their performance. We outline a comparative analysis for the same.

Keywords— MANETs, Routing Attacks, Delay, Overhead, Zones

I. INTRODUCTION

Mobile Adhoc Networks (MANETs) are wireless networks consisting of mobile nodes that communicate with each other without the use of infrastructure, thereby, making it cost effective. Such network has a decentralized approach. Each node in MANET can act as a router and thus able to communicate with each other within transmission range. Further, for nodes beyond transmission range, the intermediate nodes enable the communication. For example, in Fig. 1 nodes are communicating with each other through intermediate nodes. These networks provide applications in taxi cab network, sports stadiums, emergency rescue operations, military battlefields [1] etc.

MANETs provide various routing protocols which can be categorized into two ways *i.e.*, *proactive* and *reactive* routing. In proactive routing, information about the nodes is maintained in the routing table. Nodes in the network periodically exchange topology information, and any change in the route needs to be reflected in the routing table. While in reactive routing, also known as on demand routing, route's information is needed only when required. In addition to this, there is another routing which utilizes the benefits of both proactive and reactive routing which is termed as, *hybrid* routing.

Despite being so much resourceful, MANET has some problems like dynamic nature, absence of central check and scalability issues. Due to versatile and dynamic nature of MANETs as well as its vulnerability to various attacks, security is a major concern [3], [21]. Since nodes are continuously moving, the route which is no more available in the network remains in node's routing table. The false route entry in the routing table is termed as decayed route. Hence, the false entries about decayed routes incur routing overhead.

The paper consists of three sections. Section III describes routing protocols in MANET, Section IV provides security issues in MANETs and Section V describes attacks in MANET.

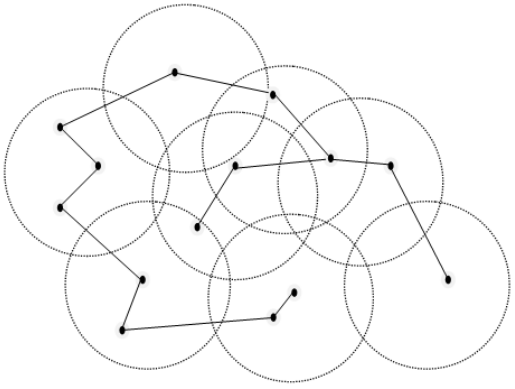

Fig. 1 Routing in MANET

© 2015, IJARCSSE All Rights Reserved

II. RELATED WORK

MANETs are very popular due to its infrastructure less characteristic. Despite the fact of popularity of MANET, these networks are very much exposed to attacks [3], [21], [25]. Meanwhile, various protocols have been developed to withstand these attacks.

Haas and Pearlman 2001 [6] described the query control schemes for Zone Routing Protocol (ZRP). ZRP uses hybrid approach which localizes the nodes into sub-networks (zones). In ZRP, proactive routing is used inside the zone and reactive outside the zone and is provided by Intra zone Routing Protocol (IARP) and Inter zone Routing Protocol (IERP) respectively. The nodes inside the zone use already available information in order to carry out routing. Thus, packet delay will be less as compared to reactive routing as there will be no route discovery needed. When node wants to communicate with a node outside its zone, then route discovery is invoked. The route request is being sent to the neighboring nodes which will forward the packet until the packet reaches to the destination. More delay overhead will be there. *Border-casting* technique is used by this hybrid protocol which minimizes the number of packets and time complexity. *Border-casting* technique allows the packets to be directly forwarded to peripheral nodes when destination node is present outside the zone. Hello messages are being exchanged among nodes using Neighbor Discovery Protocol (NDP). The NDP is used to discover neighbor nodes within transmission range of the nodes. The problem of multiple RREQ by node is being analyzed and query detection and termination schemes are used.

Navid Nikaein et al. 2001 [7] developed a Hybrid Adhoc Routing protocol. The protocol used the same concept of zones *i.e.*, Intra Zone and Inter Zone. The protocol provided bandwidth efficient low delay routing. In every zone the flooding is confined only to forwarding nodes. Thus, energy consumption and bandwidth utilization of non forwarding nodes gets reduced. The protocol uses the reactive routing mechanism for inter zones while Distributed Dynamic Routing (DDR) provides the proactive routing for intra zones. The protocol focuses on finding the stable route between source and destination node while reducing the overall delay.

Nidal Nasser and Yunfeng Chen 2007 [9] proposed an enhanced intrusion detection system. The intrusion system was proposed for the detection of malicious nodes and was based on watchdog technique. The Exwatchdog technique is being used to detect the misbehaving node. The Exwatchdog solved the drawback in watchdog technique *i.e.*, partitioning of network. The partitioning causes the network to be divided and thus, nodes no more able to communicate in different partitions. The key idea of this technique is to falsely report a genuine node as malicious node. Each node maintains tables where the records about the number of packets sent and received are stored. After receiving a report about the malicious nodes, the source node can send a message to the destination node to check whether the sum of the packets the two parts store is equal or not. Thus, if this sum of packets is equal, the node which has reported the nodes malicious is itself malicious. Otherwise, nodes being reported malicious do misbehave.

Bounpadith Kannhavong et al. 2007 [21] presented a survey on routing attacks. Adhoc on demand vector (AODV) and Optimized link state routing (OLSR) protocols has been discussed. Further, WormHole attack, BlackHole attack, Link spoofing attack, flooding attack has been described. Confirmation Request (CREQ) and Route Confirmation Reply (CREQ) used as solution for BlackHole attack. The two types of packet leashes have been proposed as solution for WormHole attack. Numerous solutions have been projected for these different attacks; Some solutions provide one performance parameter better while other solutions provide another performance parameter better, still they are not perfect in terms of effectiveness.

Sourav Kumar Bhoi et al. 2012 [10] proposed a CSRP (Centralized Secure Routing protocol). CSRP uses Master node which validate the nodes and establish session key between the nodes. A secret key SK is distributed among the general nodes in an area created by the third party. The third party is responsible for authenticating the nodes using the particular key. Master node and general nodes uses the same secret key SK. The secret key SK is responsible for placing the public keys e, n and hash function in master node MN and signature S in the general nodes [10]. Identification of nodes and establishing connection are the two main steps of this algorithm. Hence, these two components accomplish the secure routing in the CSRP using MN, signature etc. For example, If a misbehaving node tries to encroach into the third party network, then MN verifies whether it is a genuine node or not. On the other hand, if a genuine node tries to communicate or wants to go through the network, then node will use its key and easily validated.

Hung-Min Sun et al. 2013 [2] proposed a Collaborative Routing Protocol (CRP). In CRP, each node acts as a monitor node and is responsible for monitoring and storing the behavior of neighbor nodes. Source node can discover attackers and separate them by analyzing the behavior of neighbors. CRP uses the route discovery and route maintenance mechanism which is a reactive routing mechanism. Route record, sequence number, sender address, destination address and blacklist are stored in routing tables. The route record stores the identity of every node that has forwarded the route request packet. Routing overhead performance parameter has been calculated using CRP. CRP is mainly responsible for collusion attacks detection.

Parinaz Shahbazi 2013 [31] has presented a survey on hybrid routing protocols. Zone routing protocol (ZRP), Fisheye state routing (FSR), Zone based hierarchical link state routing (ZHLS), Landmark Adhoc routing (LANMAR), Scalable location update based routing protocol (SLURP), Hybrid ant colony optimization (HOPNET), Link reliability based hybrid routing (LRHR), Adhoc networking with swarm intelligence (ANSI) have been discussed. These protocols have been compared on the basis of parameters like whether multiple routes are there or not, route metric like shortest path, intra zone and inter zone, routing table or routing cache and communication complexity.

Jaspal Kumar et al. 2013 [12] describes the effect of BlackHole attack in MANETs routing protocols AODV and IAODV. The effect of BlackHole attack has been analyzed using performance parameters like end to end delay, overhead and packet delivery ratio. The vulnerability of two protocols AODV (Adhoc on Demand vector) and IAODV (Improved

© 2015, IJARCSSE All Rights Reserved

Adhoc on Demand Vector) have been analyzed. Simulations have been carried out to compare IAODV and AODV. According to the results in the paper, IAODV has more packet delivery ratio and less average end to end delay than AODV.

EO Ochola et al. 2013 [29] proposed an algorithm in power aware routing to minimize the energy consumption of nodes in the network. Since Due to limited battery power, various metrics have been used to reduce the energy. The protocol used the watchdog technique for detection of malicious nodes. The minimum energy consumption packet is used as metric which minimizes the total power that a packet uses while being forwarded between source and the destination node. The weakness of watchdog techniques has been utilized to draw solution for detecting black hole attack. The cluster head aided neighbor voting technique has been used to detect black hole attack. These cluster head nodes are non malicious nodes and are within transmission range of one hop with another cluster heads.

Kiranveer Kaur et al. 2014 [30] presented a comparison on reactive, proactive routing by considering throughput as performance parameter. The throughput of three protocols Optimized Link state Routing (OLSR), Adhoc on Demand Vector (AODV) and Dynamic Source Routing (DSR) has been analyzed. The OPNET 14 is used as a simulator and the simulations are carried out for applications like File Transfer Protocol (FTP), HTTP (Hyper Text Transfer Protocol), Video Conferencing on the basis of traffic load. The simulations are being carried out for 100 nodes under the high mobility of nodes and scalability. After analyzing the simulations, it was found that OLSR has maximum throughput than DSR and AODV. DSR has fewer throughputs than both of other protocols. The throughput also varies according to the different applications.

III. ROUTING

Due to mobility nature of nodes of MANET, and the dynamic network topology, effective routing protocols and security measures should be used so as to provide routes and security in the network. There are 3 types of routing protocols [14], [18], [24] which are discussed in Fig. 2:

- Proactive Routing
- Reactive Routing
- Hybrid Routing

Proactive Routing: These protocols are also known as Table-driven protocols. In this routing, information about nodes is stored in routing tables. Thus, route is available anytime *i.e.*, nodes do not need to keep on waiting for route. The node swaps topology information periodically, so they have route information any time when required. There is no route discovery delay associated with finding a new route. Due to table storage and maintenance, space overhead is more. Proactive protocols Traditional distributed shortest-path protocols are based on periodic updates high routing overhead. Some of the Proactive Routing protocols are Destination sequenced Distance Vector (DSDV), OLSR Optimized Link State Routing Protocol (OLSR), and Wireless Routing Protocol (WRP).

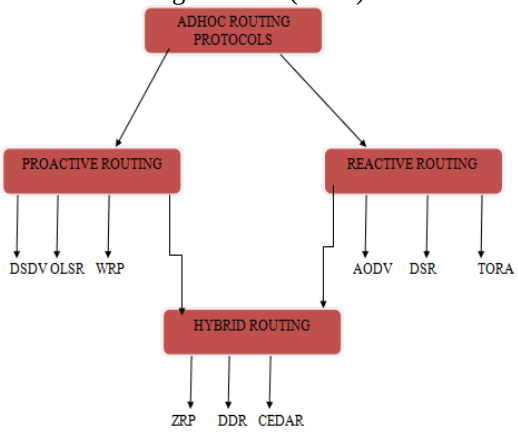

Fig. 2 Classification of routing protocols

Destination sequenced Distance Vector (DSDV): The protocol is based on classical Bellman Ford Algorithm. The information about nodes is stored and maintained in table. Every node maintains a table in which it has the node information, and information about how a node reaches to destination in terms of hops. Sequence number in this protocol is used to differentiate the decayed routes from the new ones and thus solves the problem of loop formation. Periodic updates are required to maintain the table [16].

Optimized Link State Routing (OLSR): Here, route information always stored in table. Therefore, route is always available when needed. Thus, being proactive delay is less as no waiting will be there for route discovery. Link state packets are being forwarded for topology information which is called Multi point relay (MPR). Here, each node selects its MPR from neighbor nodes. Periodic exchange of link state packets will be done in order to gather information about the nodes and their topology.

OLSR uses two types of packets:

- HELLO Message
- TOPOLOGY CONTROL (TC) Message[21]

© 2015, IJARCSSE All Rights Reserved

Hello message is used as beacon message *i.e.*, checking the presence of the neighbors and also used for MPR selection. TC message is used for route calculation.

Wireless Routing Protocol (WRP): WRP is a loop free protocol. Every node in the network uses four tables:

- Distance table(DT)
- Routing table (RT)
- Link-cost table (LCT)
- Message retransmission list (MRL) table[18]

The protocol being proactive maintains the routing information of the entire network in the tables. The protocol forces every node to perform check on consistency of predecessor information which is reported by all of its neighbors. Due to this, it faces the count-to-infinity problem.

However, the looping conditions get eliminated due to these consistency checks. Hello messages get exchanged time to time for neighbor sensing and update messages are exchanged between neighbors in case of link failures.

Reactive Routing: These protocols are also known as on demand protocols. Route is discovered here when needed. Routing is initiated by the source node using route discovery within the network. Since no information is stored, delay is more. Moreover, there is no need for periodic updates of node information. Whenever route is needed, the source node starts a route discovery phase using route request packet. The route request packet is intended to destination. Destination then sends a route reply packet to source node. After receiving route reply packet, data transmission between source and destination takes place. Due to extensive exchange of packets for route discovery, reacting routing has more delay than proactive routing. Some of the reactive routing protocols are Adhoc on Demand Vector (AODV), Dynamic Source Routing (DSR).

Adhoc On demand Vector (AODV): As the name suggests the route is made available on demand *i.e.*, when needed. AODV works very efficiently in reactive protocols. The protocol uses the route discovery and route maintenance mechanism. Thus it only needs to maintain information about the active paths [17]. Whenever a node wants to send data, it communicates by broadcasting a route request (RREQ) packet to its neighbors. Then this RREQ packet passes through the network until it reaches to its destination. Route Reply (RREP) packet is sent back from the destination to source node. AODV uses hello message to check the presence of nodes in the network [15].

Dynamic Source Routing (DSR): The protocol basically consists of two steps [21], [22]:

- Route Discovery
- Route Maintenance

Route Discovery: Since DSR is a reactive protocol, route discovery is required *i.e.*, route is made available when required. For Example, node A wants to communicate to node B, then node A will start route discovery by forwarding the packet to its neighbors. The packet will be forwarded until packet reaches to its intended destination. There will be more than one path available for the destination. The Path will be chosen based upon required condition like shortest distance, collision free.

Route Maintenance: Since nodes are continuously roaming in the network, their topology keeps changing. Thus, the alternative routes can be used. If route is not available, then route discovery is invoked. This scenario is known as Route Maintenance.

Hybrid Routing: The routing combines the features of both reactive and proactive routing. The routing reduces the delay and traffic overhead by collaborating proactive and reactive routing features. For Example: Zone Routing protocol (ZRP) [27], Zone Based Hierarchical Link State Routing Protocol (ZHLS), Core-Extraction Distributed Ad hoc Routing Algorithm (CEDAR), Distributed Dynamic Routing Protocol (DDR)[8]

Zone Routing Protocol (ZRP): The protocol is a hybrid protocol and uses the concept of zone. Every node's routing zone is described by zone radius which is expressed in terms of hops. Inside the zone Proactive Routing is used provided by Intra Zone Routing protocol (IARP). Thus routes are easily available using IARP. Outside the zone Reactive routing is used provided by Inter Zone Routing Protocol (IERP).

In ZRP, there are two types of nodes *i.e.*, the *peripheral* nodes and *interior* nodes. The peripheral nodes are nodes having minimum distance from the central node exactly equal to its zone radius. While the interior nodes are the nodes whose minimum distance from central node is less than its zone radius. For Example, in Fig. 3 the S node is central (source) node. Its zone radius=2, and F-J are its peripheral nodes and A-E are its interior nodes, K-P are nodes outside node S zone.

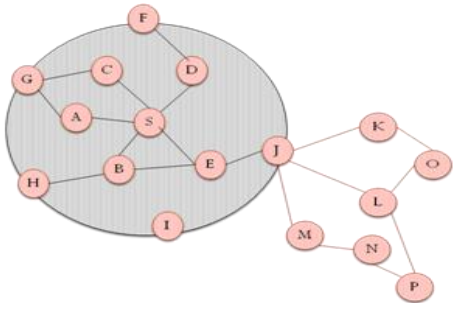

Fig. 3 Inter Zone and Intra Zones in Zone Routing Protocol

© 2015, IJARCSSE All Rights Reserved

The special feature that ZRP uses is *border-casting i.e.*, if a node wants to communicate a node which is outside its zone, then instead of broadcasting the packets it border-cast it to the peripheral (border) nodes using information provided by IARP. The border-casting technique is provided by Border-cast Resolution Protocol (BRP) [23].

Table 1 comparison of proactive reactive and hybrid routing [5], [22]

Parameters	Proactive	Reactive	Hybrid
Memory Overhead	More as table is maintained	Less as no table is maintained.	Depends whether routing is inside and outside the zone.
Availability of Route	Always available	On demand, Route Discovery will be done	Both
Delay overhead	Less as no waiting for the route	Higher than proactive as waiting for the route is there	Depend, lower when confined destinations and higher when inter zone destinations.
Network structure	Flat and Hierarchical	Flat	Mostly Hierarchical
Routing information	Stored in table	Doesn't stored information.	Inside the zone information is stored in table; outside the zone no information is stored.
Traffic control	High	Low.	Lower than both
Periodic updates of information	Required for table maintenance	Not required	Required inside the zones.
Scalability	Up to 100 nodes	Above 100 nodes	Greater than 1000 nodes
Quality of service (QoS)	Mainly focus on the route available, so less focus on QoS	Shortest route is considered in QoS support	No support

IV. SECURITY ISSUES

Nowadays Security has become the most important issue in Mobile Adhoc Networks. Security in MANETs should maintain all the security goals like authentication, access control, integrity and confidentiality. MANETs often suffers from the security attacks due to lack of centralized support, dynamic nature and open medium. Thus, these characteristics make MANETs vulnerable to various attacks [26]. With the emerging technologies, security issues also increases. MANETs works without any infrastructure i.e. any node can enter and leave the system. Thus, a malicious node will cause attacks in these networks and hence breaching security. Some of the problems In MANETs are

- Compromised Node
- Non secure Boundaries
- Infrastructure-less
- Decentralized
- Dynamic nature

V. ATTACKS

Dynamic nature, decentralized approach and infrastructure less makes MANET vulnerable to attacks [21]. There are various attacks [13], [15] that can occur in the Mobile Adhoc networks. Some of them are discussed in this paper.

- **Active Attacks:** In these attacks attacker tries to gain access to the system's data and then drop, alter and fabricate the data in order to affect the system. Such type of attacks can be easily detected as they are modifying and dropping the packets. Active attack can be external as well as internal. For example, in Fig. 4 the attacker gains access to the system and thus, sends altered messages and drop messages.

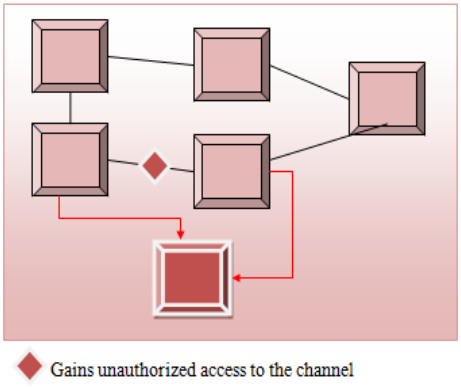

Fig. 4 in this active attack, the attacker gains access to the channel, receives packets and starts dropping them.

© 2015, IJARCSSE All Rights Reserved

- **Passive Attacks:** In these attacks, attacker only seeks information, but doesn't affect the system by using this information. The attacker listens to the channel, record patterns, analyze them. These types of attacks are difficult to detect as they are not changing data, and are not affecting the system. Encryption algorithms should be used in order to prevent these attacks. For Example, in Fig. 5 the attacker only overhears the information exchanged during the transmission of packets.

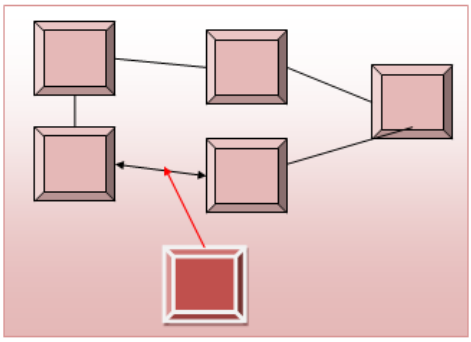

Fig. 5 passive attack scenario

- **External Attacks:** These types of attacks are done by the attacker outside the network. These attacks cause congestion, services unavailability. These attacks can be prevented by implementing security measures like firewall.
- **Internal Attacks:** These attacks are usually done by the people inside the network. Example employee in an organization can attack into security of the organization. These types of attacks are difficult to detect as the attacker has authorized access to the system.
- **Eavesdropping:** In these attacks the attacker attacks on confidentiality of the network i.e. Tries to get password, public key, private keys etc.
- **Jamming**: In these attacks the attackers firstly monitors the wireless network so that to achieve the frequency at which source and destination node are communicating. After achieving this frequency it can drop packets, block the traffic etc.
- **Routing Attacks [28]:** The malicious node attacks on the routing services and the routing protocol. Attack on these routing services will disturb the normal operations in the network and results into dropping of packets, false routes [20] etc. Attack on the routing protocol will obstruct the broadcast of routing information to a node. Routing attacks can be of various types like routing table poisoning, routing table overflow attack and routing cache poisoning attack [25].
- **BlackHole Attack [21]:** In these attacks the attacker sends false route information to the source node claiming that it has the shortest route. After establishing the route, it receives the packet from the source node. It then drops the packets and misuses these packets [4], [15]. For example, let's consider the BlackHole attack on AODV. BlackHole attack can be performed via two ways *i.e.*, Internal BlackHole Attack and External BlackHole Attack.
- **Internal BlackHole Attack:** In this attack, the malicious node is present inside the network. It enters into active data route as soon it gets the chance. The active data route is actually the route between source and destination node. Thus, after receiving the packets intended for destination, it starts dropping them. Since this type of attack uses an internal malicious node, so making it difficult to detect.
- **External BlackHole Attack:** The attack is performed by the malicious node outside the network. The malicious node firstly detects the active data route and destination node. The malicious node then forwards its RREP packet to the nearest node available in the active path. The neighbor node then forwards this packet to source node, thereby, causing updation of route entry in the routing table. Thus, malicious node receives the packet from source node and then drops the packet. For example in Fig. 6, S is source node and wants to communicate to destination D. S will forward route request (RREQ) packet to its neighbors which will further forward the packet until it reaches to destination. The malicious node G will send a RREP packet to neighbor node in active path, thereby, able to get to the source node. Thus, the malicious node will start dropping the packets.

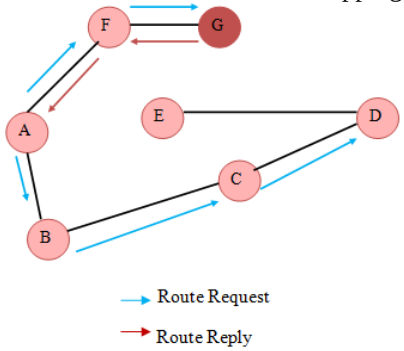

Fig. 6 BlackHole Attack on AODV

© 2015, IJARCSSE All Rights Reserved

- **WormHole Attack [21]:** The attack is also known as *tunneling* attack. In these attacks, packet is received at one point through a malicious node and then tunnels it through the other malicious node to the other point. Thus, a node sends the packet thinking that it has passed this packet through shortest route in the network [19]. For Example, in Fig. 7, Source node A wants to communicate with node M. Node A will start route discovery b y sending the route request (RREQ) packet to its immediate neighbors B and I. Malicious node C will tunnel the packet directly to malicious node F, thereby, shortening the path. Thus, M will ignore other paths and will choose the shortest path through F.

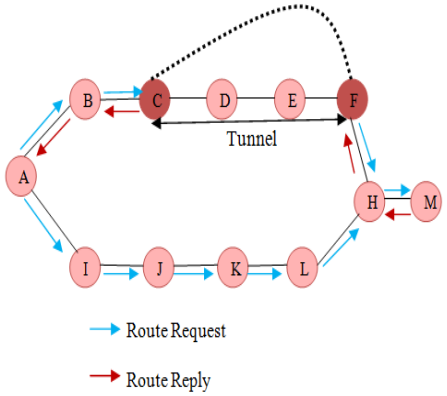

Fig. 7 WormHole Attack in reactive routing

- **Sleep Deprivation:** In these attacks the attackers makes excessive route discovery and forwards the redundant packets to the target node. Therefore, the attack causes a large reduction in battery life. The node simply goes to sleep mode in order to save the resources, when communication is halted. Since the attacker makes the nodes extremely busy, the nodes lose all of its energy and goes to the permanent sleep. Thus, the attacker easily enters into the network and exploits the rest of the network.
- **Gray Hole Attack:** In this attack, after establishing connection with the node, the attacker behaves normally in the beginning. It responds with real RREP packets to the source node. After receiving the data packets, it starts dropping them and starts the denial of service attack [11].

VI. CONCLUSIONS

The paper presents an analysis of various attacks in routing protocols in order to assess their impact in MANET environment. Despite being resourceful, MANETs are highly prone to attacks. These attacks affect MANET's integrity, confidentiality and authenticity, thereby, degrading overall performance of the network. We consider Proactive, Reactive and Hybrid routing protocols and analyzed the types of attacks in the same. The paper focuses on the consequences of various attacks in routing protocols. The future work focuses on the design of secure routing protocol and its validation through comparison with the existing protocols.

ACKNOWLEDGMENT

I would like to express my deepest gratitude to Assistant Professor Poonam Saini who has always been sincere and helpful and has guided me through the entire research. I would also like to thank my friends who have always encouraged me during the research.

REFERENCES

[1] Jaroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges" Journal of Computing 3(3). pp. 60-66, 2004

[2] Hung-Min Sun , Chiung-Hsun Chen ,Chih-Wen Yeh , Yao-Hsin Chen "A collaborative routing protocol against routing disruptions in MANETs," Pers Ubiquit Comput, vol. 17, pp 865-874, 2013

[3] P.V.Jani, "Security within Ad-Hoc Networks," Position Paper, PAMPAS Workshop, 2002

[4] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand BlackHole Attack.," CIS '09 Proceedings of International Conference on Computational Intelligence and Security, vol. 02, pp. 421-425, 2009

[5] Ritika and Malkeet Singh "Malicious Attacks and Routing Protocols in MANET: A Survey," International Journal of Electronic and Electrical Engineering, vol. 7, Number 7 pp. 743-748 , 2014

[6] Z. J. Haas and M. R. Pearlman," "ZRP: a hybrid framework for routing in ad hoc networks", Ad hoc networking, pp. 221-253, 2001

[7] Navid Nikaein, "HARP - HYBRID AD HOC ROUTING PROTOCOL", 2001

[8] N. Nikaein, H. Labiod, and C. Bonnet, "DDR: distributed dynamic routing algorithm for mobile ad hoc networks," in: First Annual Workshop on Mobile and Ad Hoc Networking and Computing, MobiHOC, pp. 19–27, 2000

[9] Nidal Nasser and Yunfeng Chen "Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks," IEEE International Conference on Communications, pp. 1154-115, 2007

© 2015, IJARCSSE All Rights Reserved

[10] Sourav Kumar Bhoi, Imran Hossain Faruk, Pabitra Mohan Khilar "CSRP: A Centralized Secure Routing Protocol for Mobile Ad Hoc Network," Third International Conference on Emerging Applications of Information technology (EAIT), pp. 429-432, 2012

[11] C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks," Second International Conference on Communications and Networking in china, pp.366-370, 2007

[12] Jaspal Kumar, M. Kulkarni, Daya Gupta, "Effect of BlackHole Attack on MANET Routing Protocols," I. J. Computer Network and Information Security, pp. 64-72, 2013

[13] HyoJin Kim, Ramachandra Bhargav Chitti and JooSeok Song, "Handling Malicious Flooding Attacks through Enhancement of Packet Processing Technique in Mobile Ad Hoc Networks," Journal of Information Processing Systems, vol. 7, pp. 137-150, 2011

[14] Nurul I. Sarkar, Wilford G. Lol, "A Study of MANET Routing Protocols: Joint Node Density, Packet Length and Mobility", IEEE symposium on Computers and Communications (ISCC), pp.515-520, 2010

[15] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma,"A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks,"JOURNAL OF COMPUTING, vol. 3, Issue 1, 2011

[16] Basu Dev Shivahare, Charu Wahi , Shalini Shivhare "Comparison Of Proactive And Reactive Routing Protocols In Mobile Adhoc Network Using Routing Protocol Property" International Journal of Emerging Technology and Advanced Engineering, vol. 2, Issue 3, 2012

[17] Meenakshi, Vinod Kumar Mishra, Kuber Singh "Simulation & Performance Analysis of Proactive, Reactive & Hybrid Routing Protocol," International Journal of Advanced Research in Computer Science and Software Engineering , vol. 2, Issue 7, 2012

[18] Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma, "Review of Various Routing Protocols for MANETs," International Journal of Information and Electronics Engineering, vol. 1, No. 3, 2011

[19] Priyanka Goyal, Vinti parmar, Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application ",IJCEM International Journal of Computational Engineering & Management, vol. 11, 2011

[20] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing security in wireless ad hoc networks," Communications magazine ,IEEE ,vol. 40, Issue 10, pp. 70-75, 2002

[21] Bounpadith Kannhavong, Hidehisa nakayama, Yoshiaki nemoto, and Nei kato, "A survey of routing attacks in mobile ad hoc networks", IEEE Wireless Communications, vol. 14, Issue 5, pp.85-91, 2007

[22] Bhavyesh Divecha, Ajith Abraham, Crina Grosan and Sugata Sanyal, "Analysis of Dynamic Source Routing and Destination-Sequenced Distance-Vector Protocols for Different Mobility models" First Asia International Conference on Modeling and Simulation, pp. 224-229, 2007

[23] Nicklas Beijar, "Zone Routing Protocol (ZRP),"Networking Laboratory, Helsinki University of Technology, P.O. BOX 3000, FIN- 02015 HUT, Finland.

[24] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani,"A Survey of Secure Mobile Ad Hoc Routing Protocols," IEEE COMMUNICATIONS SURVEYS & TUTORIALS, vol. 10, NO. 4, 2008

[25] K.P.Manikandan, Dr.R.Satyaprasad and Dr.K.Rajasekhararao, "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks" (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 2, No.3, 2011

[26] Praveen Joshi, "Security issues in routing protocols in MANETs at network layer," Procedia Computer Science 3, pp. 954–960, 2011

[27] Dhanya Sudarsan and Jisha G, "A Survey on various Improvements of Hybrid Zone Routing Protocol in MANET" ICACCI: 1261-1265.

[28] 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, vol. 2, Issue (3).

[29] EO Ochola MM Eloff, JA Van Der Poll, "The Failure of WatchDog Techniques in MANET Security: A Case of an Intelligent Black Hole".

[30] Kiranveer Kaur, Surinderjit Kaur, Vikramjit Singh"Throughput Analysis of Proactive and Reactive MANET Routing Protocols," International Journal of Emerging Research in Management &Technology ISSN: 2278-9359, vol. 3, Issue-3, 2014

[31] Parinaz Shahbazi, "A Survey on hybrid routing protocols in MANET," International Journal on Recent and Innovation Trends in Computing and Communication vol.1, 2013

© 2015, IJARCSSE All Rights Reserved