Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.7, No.2, 2016

The Modified Secure AODV Routing Protocol for Black Hole Attack in Manet

Sachin Gour[1] Prof. Sumit Sharma[2]
1.PG scholar, CSE, VIST, Bhopal, INDIA
2.HOD, CSE department , VIST, Bhopal, INDIA

Abstract
Mobile Adhoc Network is gathering of portable nodes which are actively structuring a momentary network without utilizing any pre accessible network infrastructure or central management. Each node in MANET not only provides as a specific terminal but also performs as a router to form a route. While a source node plans to send data to an intended node, packets are moved from the middle nodes. An Adhoc routing protocol is a classical method that supervises how nodes opt any route and in which manner they have to route packets among computing devices in a MANET. Because of different factors with lack of infrastructure, deficiency of already established trust relationship among the various nodes and dynamic topology, the MANET routing protocols are weak to different routing attacks. In contrast to conventional wired networks, such type attacks are executed simply in MANET because of the unsupervised entrance to the wireless medium. The malicious exploitation of various routing information results in the diffusion of wrong routing information which could eventually guide to network failure. One of these attacks in the existing wireless routing protocol like Ad-hoc on demand Distance Vector (AODV) Routing protocol is the Black Hole Attack against network truthfulness. In this attack, the data packets doesn't arrive at the destination node, thus data loss happens. There is number of detection and protection methods to reduce the intruder that achieve the black hole attack. Therefore, this paper proposes Modified Secure AODV routing protocols (MSAODV) found on threshold evaluation and cryptographic verification. In this paper, the black hole attack and the proposed MSAODV protocols are simulated in the Network Simulator NS-2 under different MANET circumstances and their performances are evaluated on various parameters like Packet drop ratio, routing overload, throughput etc.
Keywords: AODV, Black hole, gray hole, worm hole attack, MANET, AOMDV

1. INTRODUCTION

The Mobile AdHoc Networks (MANETs) is vital element of today's revolution in technology. MANETs are groups of wireless nodes that communicate by transmitting packets to others or on behalf of an additional node, without any central network management organizing data routing. In MANETs, every node performs as router or network manager for further nodes. MANETs are weak due to their fundamental features which comprise topological modification, no point of network administration, limited resources, any centralized authority, etc. Threats to personal and company privacy, and assets by attacks upon networks and computers continue in spite of efforts of network administrators and IT vendors to safeguard such environments.

Secured transmission and communication in MANET is a major challenge as this network is vulnerable to numerous kinds of attacks. Understanding of probable detection and prevention methods to MANETs is a serious matter as they are targeted by attacks [1] including Black hole attack, Denial of Service (DoS), Flooding attack, Impersonation attack, Routing table overflow attack, Selfish-node misbehaving, Wormhole attack etc. previous studies disclose the various attack classifications on MANETs like Active and Passive attacks, External and Internal attacks, and Packet Forwarding and Routing attacks. Several of the attacks seek at particular node while others seek at multiple nodes. Malicious and selfish nodes are additional kinds of attack which rigorously humiliate the security and efficiency of the network.

The present existing routing protocols are mostly classified as proactive and reactive routing protocols. In proactive routing protocol, each node proactively looks for routes to adjacent nodes. The nodes, periodically, interchange routing packets, in order to make sure the accuracy and originality of the information about routing table. DSDV (Destination Sequence Distance Vector) [2] and OLSR (Optimized Link State Routing Protocol) [3] are two most admired proactive routing protocols for MANETs. Every node in a MANET is restricted to a definite power and bandwidth, thus, constant broadcast of routing packets would direct to blocking of the network.

In MANET the reactive routing protocol, search and established a route only while two nodes mean to transfer data. Therefore, it is further known an on-demand routing protocol. Usually utilized on-demand routing protocols are AdHoc On-Demand Distance Vector (AODV) [3] and Dynamic Source Routing [4]. The multipath addition to the well known single path routing protocol AODV [5] is named as AdHoc On-demand Multipath Distance Vector (AOMDV). Both the AODV and AOMDV routing protocols depend upon support among nodes due to the lack of a centralized management and presume all nodes are reliable and well-behaved. In these routing protocols, the source node always decides the new route through route discovery. The freshness of the route is determined by the value of the sequence number. The higher the sequence number is the fresher route. However,

in an unfriendly situation, a malicious node can start routing attacks to interrupt routing operations.

MANETs work exclusive of any centralized management where the nodes communicate with all other nodes on the base of common trust. This typical feature creates MANET more defenceless to be exploited by an attacker within the network [7]. Wireless channels also create the MANET more vulnerable to attacks which produce it easier for the attacker to access within the network and acquire access to the current communication. These challenges in securing the data and improving the efficiency of communication in AdHoc network could be an open new research domain for approaches and solutions. The prime ambition of this research paper is to study various secure on-demand routing protocols for data transmission under Black Hole attack in MANET. The proposed protocols should be capable in terms of Packet drop ratio, routing overload, throughput etc. On the basis of enthusiasms to offer novel security characteristics to be included in admired routing protocols like AODV and AOMDV, the ambition is to attain the above impetus.

Rest of the paper is organized as follow: section 2 gives a brief overview of attacks on MANET, in section 3 different routing attacks in MANET is explained, in section 4 different research done by various scientist as literature survey is described, in section 5 we explain our proposed algorithm MSAODV, result analysis of our proposed algorithm is present in section 6 and finally we conclude our paper in section 7.

2. OVERVIEW OF MANET ATTACKS

The attacks in MANET mainly categorized in two major types, known as active attacks and passive attacks [8] [9]. A passive attack attains information exchanged in the network exclusive of disrupting the operation of the communications, though an active attack involves data interruption, alteration, or production, thus disrupting the usual functioning of a MANET.

Illustrations of passive attacks are eavesdropping, traffic analysis, and traffic monitoring and illustrations of active attacks comprises impersonating, jamming, modification, denial of service (DoS), and message replay. The passive attacks can be defeat by utilizing powerful encryption methods, thus making it unfeasible for eavesdroppers to acquire any constructive data from the information overheard, while the active attacks are extremely complicated to overcome.

These active attacks could be further categorized in two types, known as External attacks or Outsider attacks and Internal attacks or Insider attacks, as stated by the field of the attacks. External attacks are achieved by nodes that don't associate to the field of the network. Such attacks can be prohibited by utilizing powerful encryption methods and firewalls.

Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are harsher while contrast with outside attacks while the insider knows precious and confidential information, and owns privileged entrance rights. This node attempts to accumulate security details and could access the sheltered rights of the network. While the compromised node is an approved one in the network, it is extremely hard to recognize the internal attacks. Attacks could also be categorized according to network protocol stacks. Figure 1.2 shows the precise categorization of security attacks in MANETs [10].

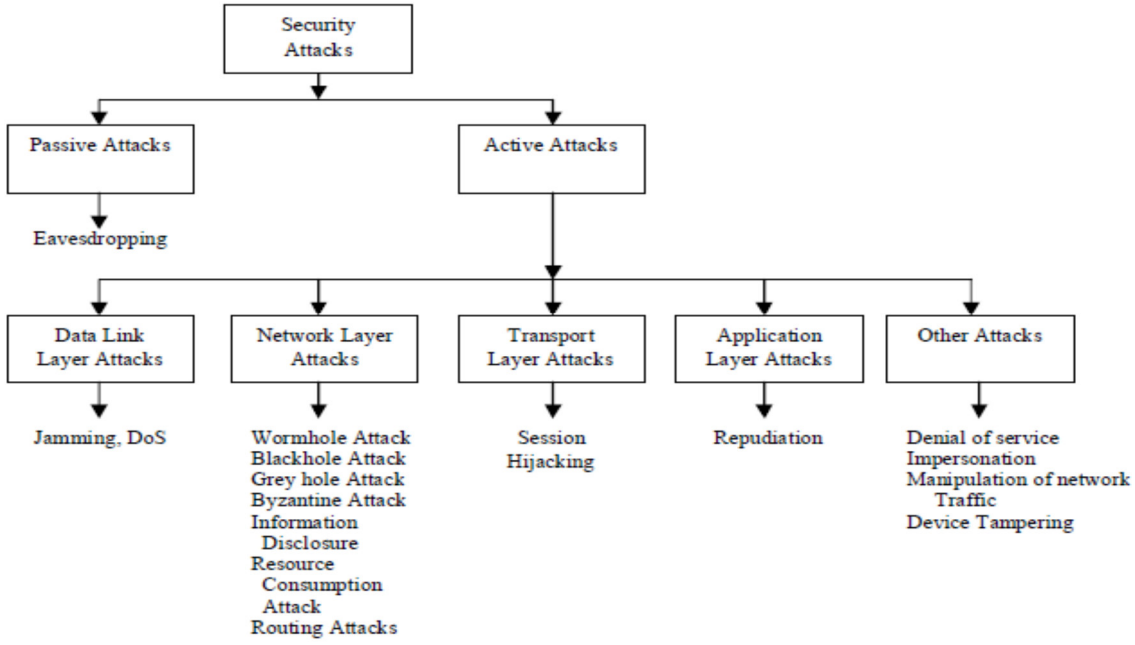

Figure 1: Classifications of Attacks in MANETs

3. ATTACKS AGAINST ROUTING

Routing is one of the major essential mechanisms in any communication like the AdHoc networks. Inappropriate and anxious routing methods will not only humiliate the performance of the AdHoc networks, but as well will provide such networks susceptible to various security attacks. One of the essential elements in the routing method is the routing packets, which is utilized to set up and maintain relationships among nodes in the networks. The significance of the routing packets has made it a major target by the attackers to launch attacks against the AdHoc networks [11] [12]. Attacks against routing packets are categorized based on the location and characteristics of attacks. The categorizations are demonstrated in Figure 1.3.

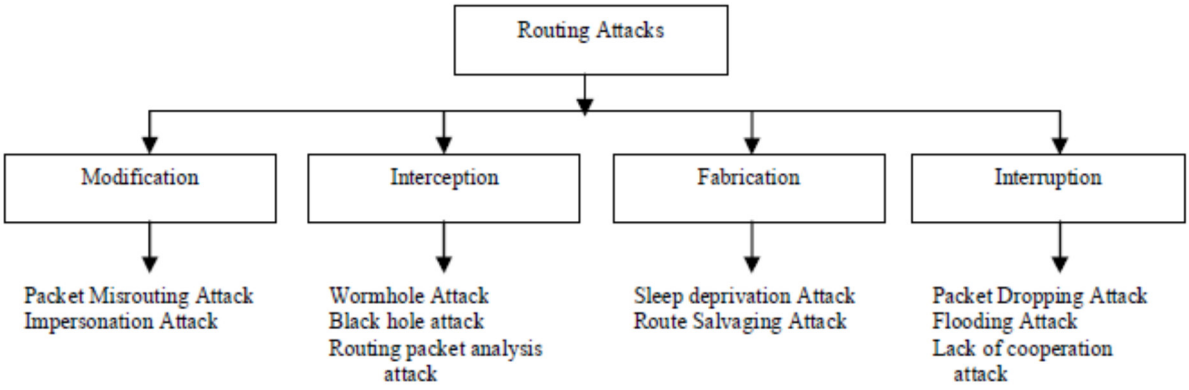

Figure 2: Classifications of Routing Attacks

In such categorization, data or packets can be deviated from the usual operation flow utilizing modification, interception, interruption or fabrication attacks. In an additional harsh case, attackers as well might utilize any combination of these attacks to interrupt the standard information flow [13].

4. LITARETURE SURVEY

There exist numerous suggestions that effort to architect a safe routing protocol for AdHoc networks to propose defence against security attacks on MANETs. These suggested solutions are either entirely new individual protocols, or in several cases incorporations of security methods into existing protocols (i.e. AODV and DSR). A general design standard in every the examined proposals have a trade off equilibrium among performance and security. Since routing is an important function of AdHoc networks, the included security process should not delay its operation. Another significant element of the study is the examination of the assumptions and the requirements on which every solution depends. As could be seen, the design of these solutions focuses on providing countermeasures against precise attacks, or set of attacks.

The Authenticated Routing for Ad hoc Networks (ARAN) protocol was advice in [14] as an individual solution for security routing in MANETs in an on demand routing fashion based on AODV. ARAN attains security ambitions of verification and non denial through the use of cryptographic certificates. ARAN could be said to consist of three operational phases. The first phase is the certification procedure that needs the existence of a trusted certification authority (CA). The second operational phase of the protocol is the route discovery procedure which offers end to end verification. This guarantees that the planned target was reached. The target node ultimately receives the RDP and replies with a reply packet (REP). The REP includes the address of the source node, the destination's certificate, a nonce and the associated timestamp. ARAN guarantees end to end verification, replay attack defence, and non denial but at the price of a somewhat higher latency.

The Secure Routing Protocol (SRP) is a set of security expansions that could be applied to any Ad hoc routing protocol that utilizes broadcasting as its route querying technique [15]. DSR is particularly preferential as the suitable protocol for incorporating the projected security extensions by the instigators of SRP. The operation of SRP needs the existence of a security association (SA) among the source node initiating a route query and the target node. A shared secret key among the two (source node and destination) is utilized by SRP of which the security association (SA) can be used in set up it.

Secure Efficient Ad hoc Distance Vector Routing (SEAD)

This is a secure Ad hoc network routing protocol based on the design of the Destination Sequenced Distance Vector (DSDV) algorithm [2]. The SEAD routing protocol utilizes the use of hash chains to validate hop counts and sequence numbers. Creating a hash chain is by applying frequently a one way hash function to a random value. The factors of such a chain are utilized to safe the updates of the routing protocol. SEAD needs the existence of a verification and key distribution system in order to validate one component of a hash chain among two nodes. With this authentic component, a node is capable to authenticate later components in the chain [16]. The SEAD

routing protocol suggests two different techniques in order to validate the source of every routing update. The first technique needs clock synchronization among the nodes that contribute in the AdHoc network, and utilizes broadcast verification methods such as TESLA [16]. The second technique needs the existence of a shared secret among every pair of nodes. This secret could be used in order to utilize a message authentication code (MAC) among the nodes that should validate a routing update message.

ARIADNE

It is a secure on demands AdHoc routing protocol. Security in Ariadne [17] follows an end to end approach, whereas the SEAD protocol utilizes hop by hop security methods [16]. Ariadne is based on DSR and developed by the instigators of the SEAD. It supposes the existence of a shared secret key among the nodes and utilizes a message authentication code (MAC) in order to validate point to point messages among these nodes [18]. Also, Ariadne utilizes the TESLA broadcast authentication protocol to validate broadcast messages such as route requests. Therefore, time synchronization is an absolute requisite of AdHoc networks that utilize Ariadne. The Ariadne protocol too specifies a method for securing route maintenance. This is attained by a node generating a route error message to inform broken links whereas including TESLA authentication details in the message. Therefore, each node that forwards the route error to the target of the message is capable to validate it [19].

The secure routing protocols that fall in hybrid type employ both symmetric and asymmetric cryptographic operations. The main frequent approach is the employ of digital signatures to give integrity and verification and also MAC, hashing and encryption to defend the metric.

Secure Ad hoc On-demand Distance Vector (SAODV) is a suggestion for safety extensions to the AODV protocol [20]. It uses digital signatures and hash chains to secure AODV packets. Cryptographic signatures are utilized for authenticating the non variable fields of the messages, while a new one-way hash chain is created for every route discovery process to secure the hop-count field in an AODV message. SAODV requires the existence of a key management mechanism that enables a node to acquire and verify the public key of other nodes.

The algorithm proposed by the authors [21] states the black hole attack in a MANET is identified based on the pre processor entitled as Pre_Process_RREP and it is easy and doesn't modify workings of either middle or target node. It doesn't still change the working of usual AODV protocol. The procedure carries on to recognize RREP packets and initiates a process entitled Compare_Pkts (packet p1, packet p2) which really evaluates the target sequence number of two packets and chooses the packet with higher target sequence number if the variation among two numbers is not considerably high. Packet holding remarkably higher target sequence number is doubted to be a malicious node and a warning message holding the node recognition is produced which is broadcasted to the adjacent nodes so that it might be isolated from the network and might sustain a list of such malicious nodes. This clarification has additional network delay and can't identify supportive black hole nodes.

In [22] authors have recommend a technique to discover the protected routes and avoid the black hole nodes (malicious node) in the MANET by verifying whether there is a huge variation among the sequence number of source node or middle node who has sent back first RREP or not. Usually, the initial route reply will be from the malicious node with higher destination sequence number, which is stored as the primary entrance in the RRTable. Then evaluate the initial destination sequence number with the source node sequence number, if there exists much more variations among them, definitely it is from the malicious node, instantly eliminate that access from the RR-Table. The suggested method can't find multiple black hole nodes.

In [23] authors suggested a method for defensive against a cooperative black hole attack. This suggested method modifies the AODV protocol by introducing two ideas, such as data routing information (DRI) table and cross checking. In the suggested method, the nodes that react to the RREQ message of a source node through route detection procedure send two bits of additional information. Every node retains an extra DRI table. In the DRI table, the bit 1 sets for "true" and the bit 0 sets for "false". The first bit "From" sets for the information on routing data packet from the node, while the second bit "Through" sets for information on routing data packet during the node.

In [24] suggested a novel protocol and customized the performance of the AODV by offering a data structure referred as trust table at each node. This table is answerable for holding the addresses of the trustworthy nodes. The RREP is expanded with an additional field known as trust field. In order for a node to be added to the trust table of another node, it needs initially to pass the behavioural analysis filter. Once the performance of the broadcasting node is normal, it is added to the trust table of the receiving node. RREP is overloaded with an additional field to specify the trustworthiness of the replying node. The cost of the trust field is initialized to zero by the replying node and may be customized by its earlier hop through the trip of the RREP. The cost of the trust field might be customized either to 2 if the replying node is the destination itself or to 1 if the replying node is not the destination but still exists in the trust table. Upon receiving RREP by the source node, it chooses whether to send the data or to wait for further route. In case the trust field cost equals to 1 or 2, the source node sends the data, otherwise the source node waits for additional route. Although the proposed technique gives trustworthy routes but it consumes high network delay.

In [25] recommend a key based on Intrusion Detection using Anomaly Detection (IDAD) to avoid attacks by both the single and multiple black hole nodes. IDAD supposes each action of a user that might be monitored and anomaly activities of an intruder might be recognized from normal activities. To discover a black hole node IDAD requires to be gives with a pre assembled set of anomaly activities, known as audit data. Once audit data is assembled, it is specified to the IDAD scheme, which is able to evaluate each action with audit data. If any action of a node is out of the action listed in the audit data, the IDAD system cut offs the particular node from the network. The reduction of the number of routing packets in turn minimizes network overhead and facilitates a faster communication.

In [26] have discussed about the AODV protocol suffering from black hole attack and recommend a feedback solution which reasonably reduces the amount of packet loss in the network. The black holes by investigative the number of sent packets at that node which will always be equivalent to zero for most of the cases. After the malicious black nodes have been identified, a feedback technique might be accepted to avoid the receptance of incoming packets at these black holes. The packets coming at the instant earlier nodes to black nodes are propagated back to the sender and the sender follows a substitute securer route to the target. However, it can't identify black hole nodes while they work as a group.

5. PROPOSED METHOD

Route detection is a weakness of AdHoc Multipath protocol that a malicious node could obtain to act as an attacker on MANETs. A malicious node in the wireless network produces a Request Reply (RR) to source nodes by sending a fake Route reply (RR) message that engage exclusive frame to be support for packet receiving to target nodes. After support (through forwarding a fake Route reply (RR) to declare it has a method to a reach preferred node) to source node that it will send data, a malicious node undertake to hold all the web commerce it.

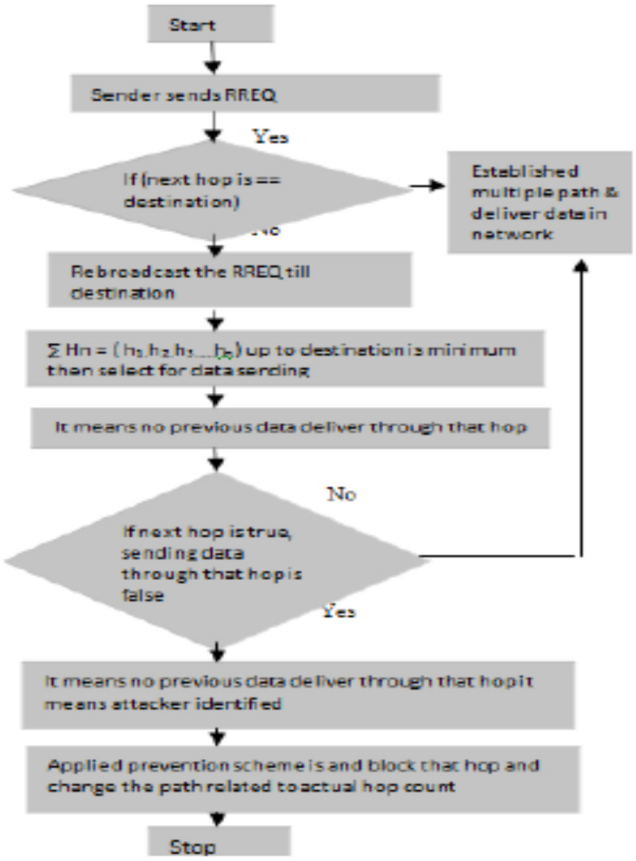

Fig.3. shows that proposed flow chart of algorithm

Trustworthy interconnection has been developed middle source nodes to desired nodes. The proposed Modified Secure AODV (MSAODV) routing algorithm finds out some path from source node to destination node using multipath routing algorithm. After determine some paths, all the paths are classified which rely on the estimation characteristic of appearance of attacker. Then it would refer the improved paths which will groups no emergence of malicious attacker. In this algorithm the data is secure in existence of IDS format. Then it sends the data on improved single channels of some identified route in Mobile AdHoc network.

We utilize the Proposed MSAODV algorithm to find out the multi paths from source node to destination

node by utilizing multipath routing algorithm. After identifying multi paths, all the paths are separated on the basis of sentence component of appearance of attacker in paths. Then it would refer the improved paths that will posses no possibility of malicious attacker. Then it sends the data via improved single path of some developed path in network. In this algorithm the data is secure in presence of IDS. In this paper we analyze three modules of routing:

1) **Normal Module:** To evaluate the present AODV protocol without attack.
2) **Attack Module:** To evaluate the present AODV protocol with attack.
3) **MSAODV Module:** This module is proposed to provide security in presence of black hole attack. The attackers are completely achieving no routing awful performance and provide suitable routing. The whole approach of security algorithm is disclosed upcoming extremity.

Flow Graph of Proposed algorithm: The flow graph of proposed MSAODV is presents in fig. 3. The phases to detect the attacker and hold the identities of attacker by that secure communication in practical.

6. RESULT ANALYSIS

The three modules i.e. normal, Attack and MSAODV algorithm against malicious attack is implemented on open source simulator NS-2.3. The Tcl of width imitated for 20, 40, 60, 80 and 100 nodes. NS duration is of 100 second. Each node has a transmission area of 250 meter. The minimum rate for the simulation is 3 m/s while the outermost rate is 30 m/s. each node in the Mobile AdHoc network is allocate primary location within the simulation range of 800×800 meters and joins the network at an inconsistent time. The packets are generating utilize file transfer protocol (FTP) and constant bit rate (CBR) with rate of 3 packets per seconds. Nodes are typically assign at beginning, and the actual location for the node is explain in a TCL file assign for the simulation utilize a part interior ns-2.3. The Propagation model is utilized two Ray Ground and the MAC surface electronics of 802.11 is consider for wireless communication. The attacker node is generating four and inimical those IDS nodes are plot in network

Performance Metrics

Table 1: performance metrics used

Topology Dimension	800m X 800m
Packet Size	512 bytes
Simulation Time	100 second
Number of nodes	20, 40, 60, 80, and 100
Routing Protocol	AOMDV
Traffic Pattern	CBR / FTP
Link Layer Type	LL
Mac Type	802.11
Radio Propagation Model	Two Ray Ground
Antenna model	Antenna/Omni

The following illustrates metrics are utilizing for difference to analysis performance:

1. **Packet Delivery Ratio (PDR):** The relationship of the packet delivered to the destination node to the data sent by the source node. The PDF signify mode of victorious a protocol illustrate forwarding data from source to destination node.
2. **Average End-to End Delay:** The average delay between the source node of data by the beginning and its obtaining by the destination node. This occupied all possible decrease reason through packet delivered, route discovery, proceeding at mediator nodes. It is measured in ms.
3. **Normalized Routing Load (NRL):** The number of normalized data delivered per data packet forward to the destination node. The routing load reduced is representing best result.
4. **Throughput:** Throughput is the medium speed of wealthy data forward over a communication link. A high average packet delivery network is sensible.

The results performance evaluates on the basis of simulation parameters used in this section.

A) Packet Drop Analysis in normal, attack & MSAODV module –

The data drop on attack at the rate of routing is the routing misbehaviour in network. The attacker is overripe to demonstrate the routing by gripping the data information in network. In the graph shown below the data drop % is evaluate in case of routing bad-behaviour of attacker. This show with nodes weight of 20, 40, 60, 80 and 100 as represent in fig 4. The drop % is reorganization from the mentioned three modules and in attack module only attacker nodes are drop the data. The drop % is about 19% at the ending of simulation. The dropper overtake by attacker is not recognizing in presence of proposed security algorithm. The MSAODV algorithm holds the attacker identities and provide attack free network.

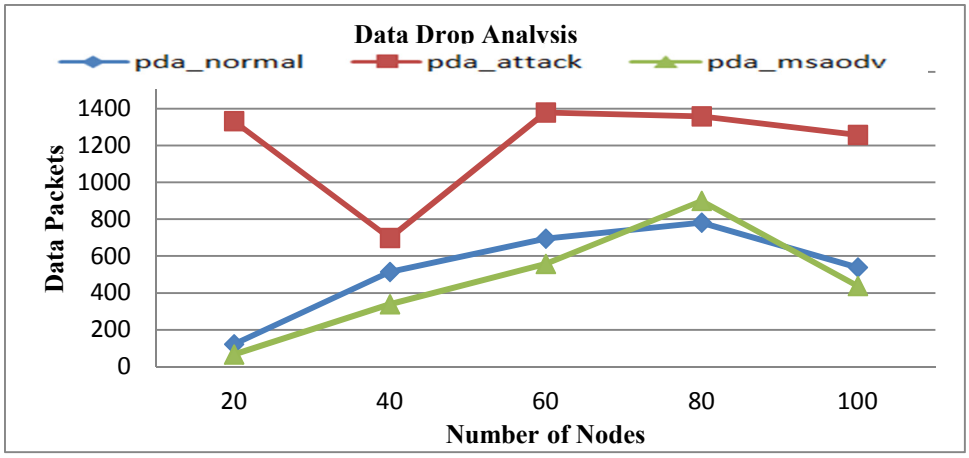

Fig.4: Packet Drop Analysis

b) PDR Analysis in normal, attack & MSAODV module

The packets successful delivered is refining the explanations of network apart from that the data dropping is minimum the performance of network. The routing misbehaviour pass by black hole attack is decrease the % of data recognizing in node of 20, 40, 60, 80 and 100 as represent in fig 5. The attacker is downs whole data packets that are not delivered to destination node following approve Route Reply. The % of data successfully delivered in case of normal, attack & MSAODV module is shows in this graph. The attacker module shows about 2 % up to simulation rate of 50 seconds. The attacker has drop the greatest amount of the data packets by that the dispel performance of multipath routing is reduced.

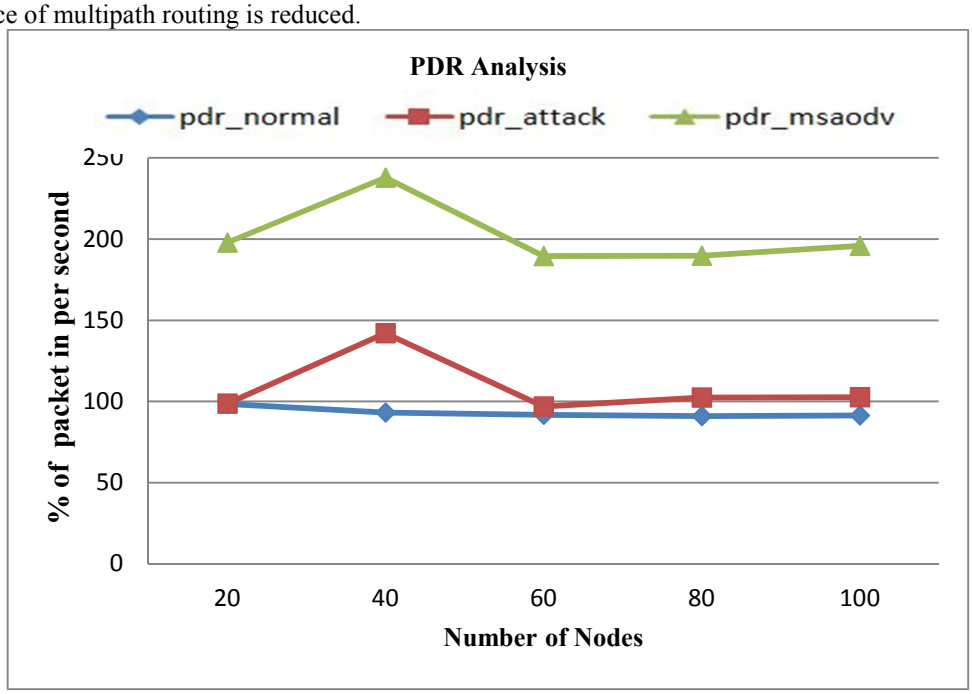

Fig.5: PDR Analysis

c). Routing Overload Analysis in normal, attack & MSAODV module

The routing overhead is specify by the number of routing packets are forward in network. The routing packets are drowning in network to improvement relationship in between source and target passes by intermediate nodes. The nodes are create critical topology by that the connect growth is the testing difficulty in MANET. The graph shows the routing overload in case of Normal, Attack, & MSAODV module and observe that the performance of MSAODV algorithm is get better the in presence of attack environment in 20, 40, 60, 80 and 100 nodes scenario as shown in fig 6.

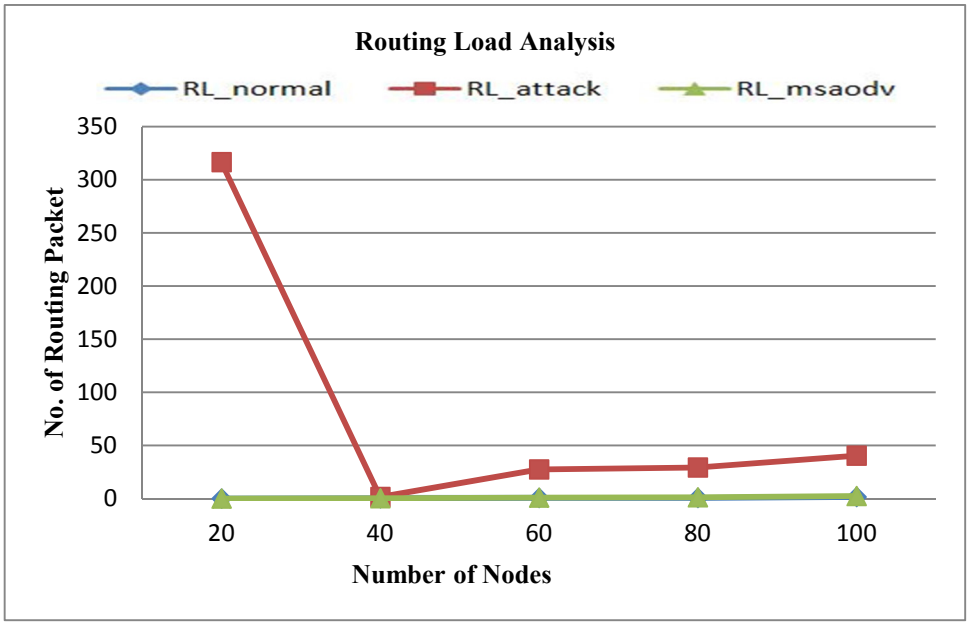

Fig.6: Routing Load Analysis

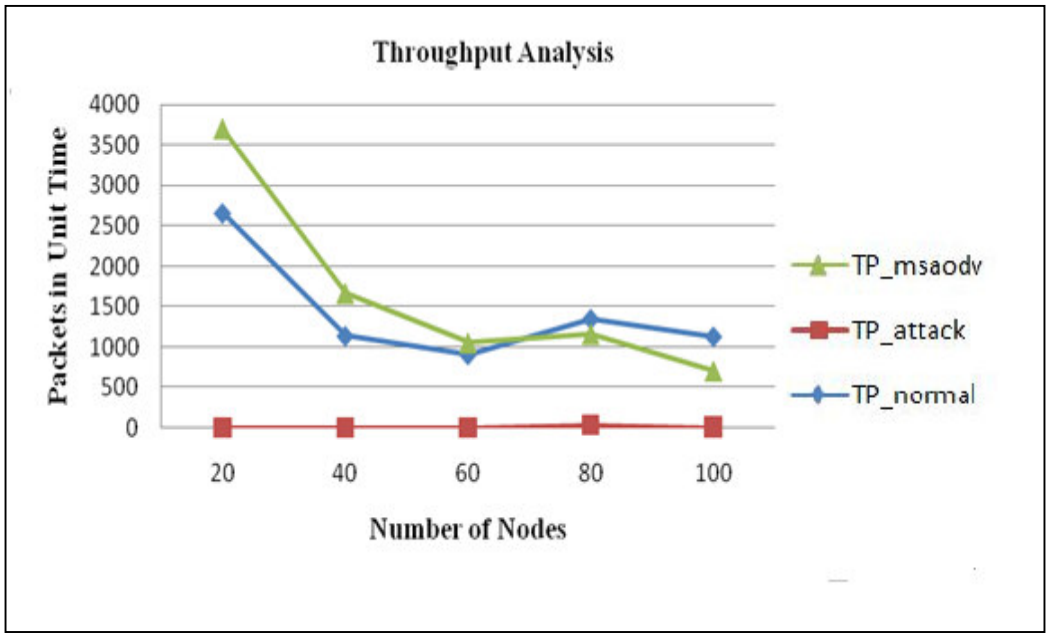

Fig.7: Throughput Analysis

d). Throughput Analysis in normal, attack & MSAODV module

The data gathering in Mobile AdHoc network is not unit on any management. The data delivery in this type of network is not safe. In this graph we demonstrate the throughput analysis in case of Normal, Attack, & MSAODV module. The data per unit of time in case of attacker is nearly small in network but in case of proposed safety algorithm the throughput is greater as compare to attacker in 20, 40, 60, 80 and 100 nodes circumstances as shown in fig 7.

7. Conclusion

The ultimate goal of this paper is to suggest solutions for safe Mobile AdHoc Network (MANET). We started our research by analyzing the major research areas of MANET security. In study we recognize that the major issues pertaining to MANET are the terms of availability, confidentiality and integrity by investigating safe routing, safe Peer to Peer overlays and intrusion detection mechanisms. Nevertheless, the typical available MANET routing protocols have insignificant or no safety methods. This creates them and MANET network extremely anxious and vulnerable to a variety of security attacks. Safe routing in AdHoc networks is the major aim of our research.

Reliability is the critical difficulty in Mobile AdHoc network. The data packets in network are forwarding among source and destination along with routing application of connection establishment. The performance is represent in 20, 40, 60, 80 and 100 nodes graph. The attacker is gripping all dropped data that are the reason of routing misbehaviour in Mobile AdHoc network. The malicious attacker movement is grip by proposed security algorithm and provides the attack free network. The multipath routing protocol like AOMDV provides the alternative to the difficulties in available route is arising. The routing performance is calculated by showing metrics in Normal, Attack, & MSAODV module. The proposed security algorithm identifies the attacker through NH information of data forwarding and as well forwards the reorganization of node recognition of attacker in network. If that recognition is appear in routes development then the different routes is opt for data forwarding. Furthermore after reject the performance of network by attack the proposed security algorithm recover 95 % of packet drop as compare to normal multipath algorithms.

Several attractive issues and unsolved difficulties that need further research have appeared in this research paper. These are briefly summarized below. In future we could also implement this security algorithm on different routing attacks like wormhole attack and Gray hole attack etc. we could also inspect the impact of attack on energy utilization in mobile nodes just because in the absence of energy nodes in MANET are not sustain for an overlong time.

REFERENCES

[1] Yang, Hao, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang. "Security in mobile ad hoc networks: challenges and solutions." *Wireless Communications, IEEE* 11, no. 1 (2004): 38-47.

[2] He, Guoyou. "Destination-sequenced distance vector (DSDV) protocol."*Networking Laboratory, Helsinki University of Technology* (2002): 1-9.

[3] Clausen, Thomas, and Philippe Jacquet. *Optimized link state routing protocol (OLSR)*. No. RFC 3626. 2003.

[4] Perkins, Charles, Elizabeth Belding-Royer, and Samir Das. *Ad hoc on-demand distance vector (AODV) routing*. No. RFC 3561. 2003.

[5] Johnson, David B. "The dynamic source routing protocol for mobile ad hoc networks." *draft-ietf-manet-dsr-09. txt* (2003).

[6] Marina, Mahesh K., and Samir R. Das. "On-demand multipath distance vector routing in ad hoc networks." In *Network Protocols, 2001. Ninth International Conference on*, pp. 14-23. IEEE, 2001.

[7] Zapata, Manel Guerrero, and Nadarajah Asokan. "Securing ad hoc routing protocols." In *Proceedings of the 1st ACM workshop on Wireless security*, pp. 1-10. ACM, 2002.

[8] Oppliger, Rolf. *Internet and intranet security*. Artech House, 2001.

[9] Yi, Seung, and Robin Kravets. "Composite Key Management for Ad Hoc Networks." In *MobiQuitous*, pp. 52-61. 2004.

[10] Murthy, C. Siva Ram, and B. S. Manoj. *Ad hoc wireless networks: Architectures and protocols*. Pearson education, 2004.

[11] Capkun, Srdjan, Levente Buttya, and Jean-Pierre Hubaux. "Self-organized public-key management for mobile ad hoc networks." *Mobile Computing, IEEE Transactions on* 2, no. 1 (2003): 52-64.

[12] Qin, Huaizhi Li Zhenliu Chen Xiangyang, Chengdong Li, and Hui Tan. "Secure routing in wired networks and wireless ad hoc networks." (2004).

[13] Kannhavong, Bounpadith, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, and Abbas Jamalipour. "A survey of routing attacks in mobile ad hoc networks." *Wireless communications, IEEE* 14, no. 5 (2007): 85-91.

[14] Yi, Seung, Prasad Naldurg, and Robin Kravets. "Security-aware ad hoc routing for wireless networks." In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, pp. 299-302. ACM, 2001.

[15] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Packet leashes: a defense against wormhole attacks in wireless networks." In *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 3, pp. 1976-1986. IEEE, 2003

[16] P. Argyroudis and D. O'Mahony, "Secure routing for mobile Ad hoc networks,"IEEE Communications Surveys & Tutorials, vol. 7, no. 3,pp. 2-21, 2005.

[17] Hu, Yih-Chun, Adrian Perrig, and David B. Johnson. "Ariadne: A secure on-demand routing protocol for ad hoc networks." *Wireless networks* 11, no. 1-2 (2005): 21-38.

[18] Ramanujan, Ranga, Atiq Ahamad, Jordan Bonney, Ryan Hagelstrom, and Ken Thurber. "Techniques for intrusion-resistant ad hoc routing algorithms (TIARA)." In *MILCOM 2000. 21st Century Military Communications Conference Proceedings*, vol. 2, pp. 660-664. IEEE, 2000.

[19] Ogier, Richard, Fred Templin, and Mark Lewis. *Topology dissemination based on reverse-path forwarding (TBRPF)*. No. RFC 3684. 2004.

[20] S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol,” RFC 2401, Nov. 1998.

[21] Mandhata, Subash Chandra, and Surya Narayan Patro. "A counter measure to Black hole attack on AODV-based Mobile Ad-Hoc Networks." *International Journal of Computer & Communication Technology (IJCCT)* 2, no. 6 (2011): 37-42.

[22] Himral, Lalit, Vishal Vig, and Nagesh Chand. "Preventing aodv routing protocol from black hole attack." *Lalit Himral et al./International Journal of Engineering Science and Technology (IJEST)* 3, no. 5 (2011).

[23] Sen, Jaydip, Sripad Koilakonda, and Arijit Ukil. "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks." In *Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on*, pp. 338-343. IEEE, 2011.

[24] Khamayseh, Yaser, Abdulraheem Bader, Wail Mardini, and Muneer Bani Yasein. "A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks." *International Journal of Communication Networks and Information Security* 3, no. 1 (2011): 36.

[25] Alem, Yibeltal Fantahun, and Zhao Cheng Xuan. "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection." In *Future Computer and Communication (ICFCC), 2010 2nd International Conference on*, vol. 3, pp. V3-672. IEEE, 2010.

[26] Singh, Herminder. "Shweta, "An approach for detection and removal of Black hole In MANETS"." *International Journal of Research in IT& Management (IJRIM)* 1, no. 2 (2011).