the next-hop list and the advertised hop count are reinitialized.

AOMDV can be used to find node-disjoint or link-disjoint routes in order to avoid active attack. To find node-disjoint routes, each node does not immediately reject duplicate RREQs. Each RREQs arriving via a different neighbor of the source defines a node-disjoint path. This is because nodes cannot be broadcast duplicate RREQs, so any two RREQs arriving at an intermediate node via a different neighbor of the source could not have traversed the same node. In an attempt to get multiple link-disjoint routes, the destination replies to duplicate RREQs, the destination only replies to RREQs arriving via unique neighbors. After the first hop, the RREPs follow the reverse paths, which are node disjoint and thus link-disjoint. The trajectories of each RREP may intersect at an intermediate node, but each takes a different reverse path to the source to ensure link disjointness. The advantage of using AOMDV is that it allows intermediate nodes to reply to RREQs, while still selecting disjoint paths. But, AOMDV has more message overheads during route discovery due to increased flooding and since it is a multipath routing protocol, the destination replies to the multiple RREQs those results are in longer overhead.

Recently, many secure multipath routing schemes were proposed to protect information security in MANET, such as however, the solutions of these schemes mainly focus on security issues, and can not be directly used for privacy protection for lack of an anonymous routing mechanism. Anonymity, as an important security requirement, should be paid much more attention in mobile ad hoc routing protocols, especially in privacy-vital environment. The anonymous routing protocol means that the scheme should protect identity of nodes, location information, data information and traffic information against an adversary who wants to collect and analyze the information for illegal act.

A. Dynamic Source Routing Protocol

The dynamic source routing (DSR) protocol is a simple and efficient routing protocol designed specifically for use in ad hoc networks of mobile nodes . The protocol is composed of the two main parts of “route discovery” and “route maintenance”. The protocol operates on demand and allows each sender to select and control the routes used in routing its packets. Other advantages of the DSR protocol include easily guaranteed loop-free routing, operation in networks containing unidirectional links and very rapid recovery when routes in the network change.

B. Hash Function

Hash function is a cryptographic algorithm which transforms an input value to a fixed-sized output value, generally, we call the hash value or the message digests. A hash function H() should have the characteristic that given an input value M, it is efficiently computable to obtain the hash value H(M). At the same time, given H(M), it is computationally difficult to get back the value M. A hash function is considered to be insecure if we find a message that matches a given hash value or exist two different messages that have the same hash value by computing H(). A hash function is used to detect the active attacks in our scheme

1) *Multipath Route Discovery :* The basic idea behind multipath route discovery is finding multiple node-/link disjoint paths to a destination node, if the active attack occurs in a single path, then the AOMDV will send the data packets in some other route which is available in the multipath routing. This is not possible in the AODV, since there exists only one path. If that single path is attacked by a active in AODV, then there are no possibilities for further transmission and many packets may be dropped. But AOMDV uses a low overhead, because flooding RREQ's through the network is being done already by AODV. Due to AODV already flooding the network, it is easy to see that a change in behavior when a node receives a RREQ can result in multiple routes to the same destination. The destination node must be allowed to send more RREP's, one for each path.

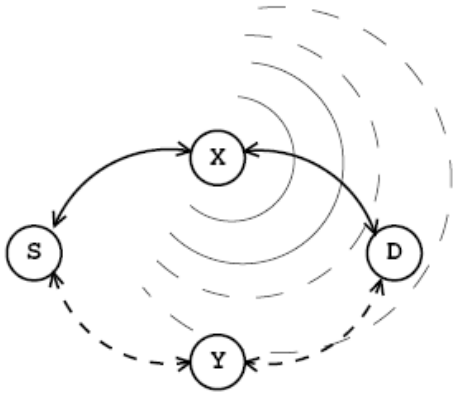

Figure 1 shows two node disjoint paths from a source to a destination. In article it’s proved how link-/node disjoint paths are discovered, and how it is implemented.

AOMDV shares several characteristics with AODV. It is based on the distance vector concept and uses hop-by-hop routing approach. Moreover, AOMDV also finds routes on demand using a route discovery procedure. The main difference lies in the number of routes found in each route discovery. In AOMDV, RREQ propagation from the source towards the destination establishes multiple reverse paths both at intermediate nodes as well as the destination. Multiple RREPs traverse these reverse paths back to form multiple forward paths to the destination at the source and intermediate nodes. Note that AOMDV also provides intermediate nodes with alternate paths as they are found to be useful in reducing route discovery frequency.

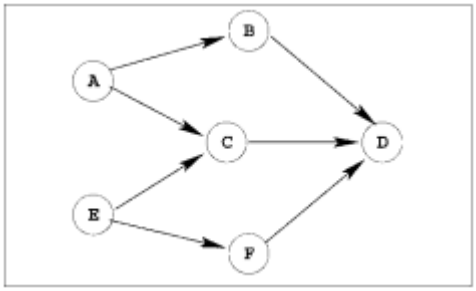

Figure 2: Paths maintained at different nodes to a destination may not be mutually disjoint

Here D is the destination. Node A has two disjoint paths to D: A – B – D and A – C – D. Similarly, node E has two disjoint paths to D: E – C – D and E – F – D. But the paths A – C – D and E – C – D are not disjoint; they share a common link C – D.

The core of the AOMDV protocol lies in ensuring that multiple paths discovered are loop-free and disjoint, and in efficiently finding such paths using a flood-based route discovery. AOMDV route update rules, applied locally at each node, play a key role in avoiding the active attacks and improve the performance and the network security.

AOMDV relies as much as possible on the routing information already available in the underlying AODV protocol, thereby limiting the overhead incurred in discovering multiple paths. In particular, it does not employ any special control packets. In fact, since the AOMDV uses multiple paths to avoid most of the active attack for extra RREPs and RERRs for multipath discovery and maintenance along with a few extra fields in routing control packets (i.e., RREQs, RREPs, and RERRs) constitute the only additional overhead in AOMDV relative to AODV.

2) *Summary:* This chapter discusses the proposed work AOMDV with Multipath routing and demonstrated how multipath routing can be added to the AODV protocol and how it will improve performance in a network with a low overhead to avoid the various attack and improves the network security.

2. Experimental Results

Implementation of wireless ad-hoc networks in the real world is quite hard. Hence, the preferred alternative is to use some simulation software which can mimic real-life scenarios. Though it is difficult to reproduce all the real life factors such as humidity, wind and human behavior in the scenarios generated, most of the characteristics can be programmed into the scenario.

To compare two on-demand ad-hoc routing protocol against the active attack, and analyze the anonymity and security features of our proposed routing protocol theoretically, it is best to use identical simulation environments for their performance evaluation.

3. Simulation Environment

NS-2 simulator is used which has support for simulating a multi-hop wireless ad-hoc environment completed with physical, data link, and medium access control (MAC) layer models on NS-2. The table 1 below shows the context of our simulation

Table 1: Simulation Set Up Parameters

Network range	2000x1000 m
Transmission Range	200m
Bandwidth	2 Mbps
Traffic Type	CBR
Packet size	512 Bytes
Number of Nodes	50

The protocols maintain a send buffer of 500 packets. It contains all data packets waiting for a route, such as packets for which route discovery has started, but no reply has arrived yet. All packets sent by the routing layer are queued at the interface queue till the MAC layer transmits them. The maximum size for interface priority queue is 50 packets and it maintains it with two priorities, each served in FIFO order. Routing packets get higher priority than data packets.

A) Performance Evaluation Metrics

The performance of AODV and AOMDV against the active attack is compared according to the following performance metrics:

Packet Delivery Ratio - The ratio of data packets delivered to the destinations to those generated by the constant bit rate. *Average End-to-End delay of data packets* - This includes all possible delays caused by buffering during route discovery, queuing at the interface queue, retransmission delays, propagation and transfer times.

Number of packets dropped - The total number of routing packets dropped during the simulation.

1) *Packet Delivery Ratio (PDR):*The simulation is done for 500sec for seven scenarios with pause times varying from 0 to 500 s. Packet delivery ratio is calculated for AODV and AOMDV. The results are summarized below with their corresponding graph.

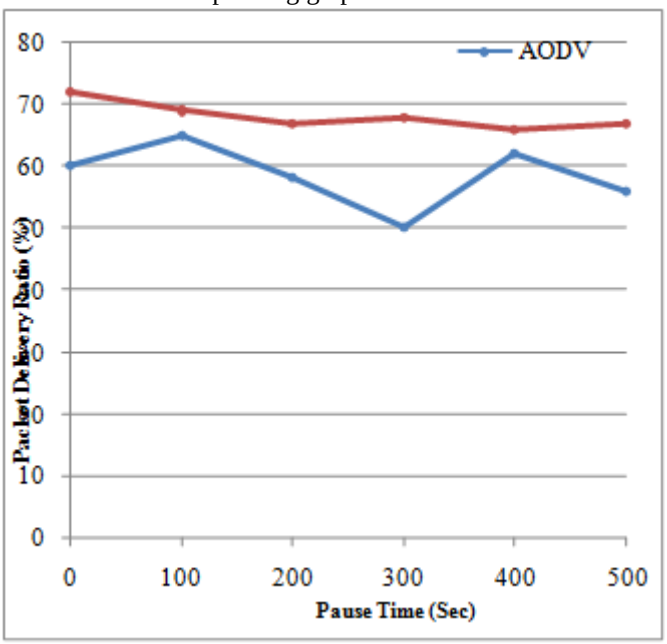

Figure 3: Comparison of AODV and AOMDV on basis of PDR

From the figure 3, it is confirmed that AOMDV has a better PDR value when compared to AODV for each set of connections.

2) *Average End-to-End delay of data packets:* From the figure 4, it is confirmed that AOMDV has very low average delay than AODV due to the fact if a link break occurs in the current topology, AOMDV would try to find an alternate path from among the backup routes between the source and the destination node pairs

resulting in additional delay to the packet delivery time. In comparison, if a black hole attack occurs in AODV, the packet would not reach the destination another path from source to destination, since only singular paths exist in AODV between a source and destination node.

dropped. But due to AOMDV being a multipath routing protocol, even if the current link breaks due to black hole attack, the network will find an alternate path from the source to the destination node and have a better chance of packet delivery without any block hole attack; hence less number of packets will be dropped for AOMDV.

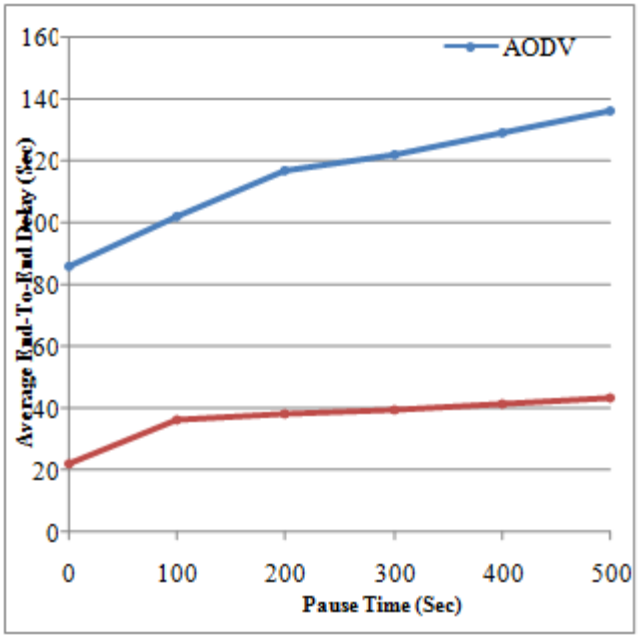

Figure 4: Comparison of AODV and AOMDV on basis of average End-to-End delay

3) **Number of Packets Dropped:** The number of packets dropped in AODV is more than the number of packets dropped in AOMDV. This is because of the fact that due to AODV being a unipath routing protocol and it is more vulnerable to black hole attack and also if a black hole attack occurs on a link, the packet will not be delivered to the destination node. Thus that packet will get

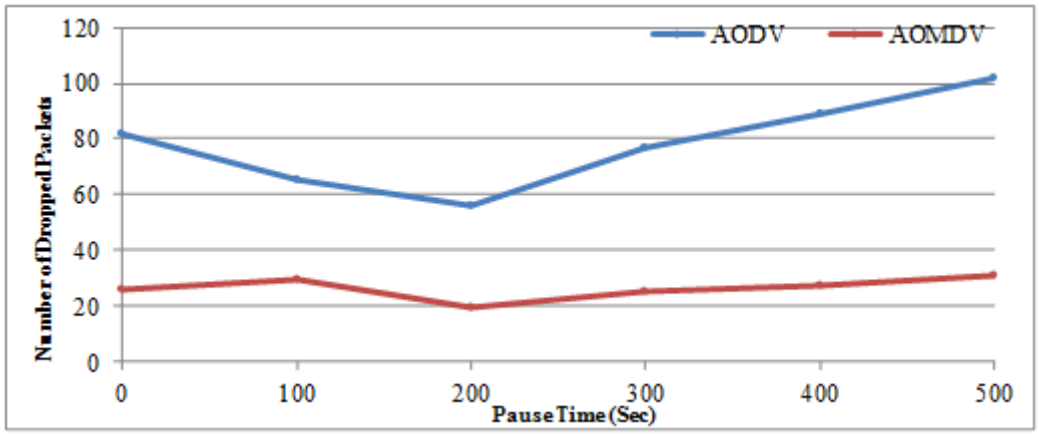

Figure 5: Comparison of AODV and AOMDV on basis of number of dropped packets

4) ***Summary:*** This chapter evaluates the performances of AODV and AOMDV against active attacks using NS-2. The comparison was based on of packet delivery ratio, average end-to-end delay and the number of packets dropped. It is found from the results, that AOMDV is better than AODV. AODV can be easily attacked by black holes due its inability to search for alternate routes when a current link breaks down but AOMDV uses multipath routing which avoids active attack and it improves the network security.

4. Conclusion

In this work, a protocol called Ad-hoc On-demand Multipath Distance Vector Routing (AOMDV) is proposed in order to avoid the active attack and thus improving the network security. The main objective of this research is to avoid the black hole attack in the MANET. AOMDV protocol provides identity anonymity, location anonymity, data and traffic anonymity by employing cryptograph technology and secret sharing in MANET communication process. Meanwhile, the protocol can effectively thwart the various

passive attacks, detect active attacks (such as tampering attack) and reduce the successful probability of physical destroy attack.

The proposed AOMDV protocol utilizes multipath routing. Therefore, when an active attack occurs in a path, the AOMDV will route the data packets in some other routes. Thus the performance of the system gets increased. The performance measures used to evaluate the proposed approach are;

- Packet Delivery Ratio
- Average End-to-End Delay
- The Number of Packets Dropped

AOMDV has better packet delivery ratio and comparatively low average end-to-end delay when compared to the existing AODV protocol. The number of packets dropped in the AOMDV against the active attack is very low. Thus the proposed AOMDV is proved to be better against the various attacks. It also improves the network security.

5. Scope for Future Work

In order to avoid the black hole Attack in the Ad-hoc Networks, AOMDV routing protocol is proposed in this work. From the simulated results, it is found that the AOMDV protocol is less prone to black hole attack than the AODV routing protocol.

- In this study, the AOMDV protocol is used to avoid the black hole attack. The other routing protocols are simulated in future in order to find the best routing protocol for minimizing the Black Hole Attack.
- A robust framework that uses minimal public key cryptography is avoided to reduce the overload on the network. Instead of public key cryptography, shared key cryptography is extensively used to provide the security against the black hole attack.

Efficient techniques should be developed to detect the black hole nodes in MANETs.

References

[1] "Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks," IEEE Trans. Vehic. Tech., Vol. 55, No. 4, Pp. 1302–1310, 2006.
[2] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology", Sweden, 2007.
[3] Li Shi-Chang, Yang Hao-Lan, Zhu Qing-Sheng, "Research on MANET Security Architecture Design", International Conference on Signal Acquisition and Processing (ICSAP '10), Pp. 90 – 93, 2010.
[4] Yang Xu, XiaoyaoXie, "Security analysis of routing protocol for MANET based on extended Rubin logic", IEEE International Conference on Networking, Sensing and Control (ICNSC), Pp. 1326 – 1331, 2008.
[5] M. Salmanian, P.C. Mason, J. Treurniet, Jiangxin Hu, Li Pan, Ming Li, "A modular security architecture for managing security associations in MANETs", IEEE 7th International Conference on Mobile Adhoc and Sensor Systems (MASS), Pp. 525 – 530, 2010.
[6] C. Li, Zhuang Wang, Cungang Yang, "SEAODV: A Security Enhanced AODV routing protocol for wireless mesh networks", IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Pp. 699 – 706, 2010.
[7] Songbai Lu, Longxuan Li, Kwok-Yan Lam, LingyanJia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", International Conference on Computational Intelligence and Security (CIS '09), Vol. 2, Pp. 421 – 425, 2009.
[8] YinghuaGuo, M. Simon, "Network Forensics in MANET: Traffic Analysis of Source Spoofed DoS Attacks", 4th International Conference on Network and System Security (NSS), Pp. 128 – 135, 2010.
[9] M. Medadian, M.H. Yektaie, A.M. Rahmani, "Combat with Black hole attack in AODV routing protocol in MANET", First Asian Himalayas International Conference onInternet (AH-ICI), Pp. 1 – 5, 2009.
[10] XiaoYang Zhang, Y. Sekiya, Y. Wakahara, "Proposal of a method to detect black hole attack in MANET", International Symposium on Autonomous Decentralized Systems (ISADS '09), 1 – 6, 2009.
[11] A. Shevtekar, K. Anantharam, and N. Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," IEEE Commun. Lett., Vol. 9, No. 4, Pp. 363–65, 2005.