Delay Efficient Authenticated Anonymous Secure Routing for MANETs

Sunetra P. Salunkhe
Master Student, Computer Engineering
S.S.V.P.S's B.S. Deore College of Engineering
Dhule, India

Hitendra D. Patil, PhD
Professor and Head, Computer Engineering
S.S.V.P.S's B.S. Deore College of Engineering
Dhule, India

ABSTRACT
The mobile ad hoc network (MANET) is nothing but the wireless connection of mobile nodes which provides the communication and mobility among wireless nodes without the need of any physical infrastructure or centralized devices such as access point or base station. The communications in MANET is done by routing protocols. At present MANET is used in many real time applications and hence such networks are vulnerable to different kinds of security threats. MANET networks suffered more from security attacks due to use of free wireless communication frequency spectrum and dynamic topology. Therefore it becomes very tough to provide secure to MANET under different adversarial environments like battlefields. For MANET, anonymous communications are vital under the adversarial environments, in which the identification of nodes as well as routes is replaced by pseudonyms or random numbers for the purpose of protection. There are many protocols presented for anonymous communication security for MANET, however suffered from limitations like worst delay, vulnerable to DoS attacks etc. In this paper presents Delay Efficient Authenticated Anonymous Secure Routing [DEAASR] which is extension of existing AASR approach presented recently. The main aim of DEAASR protocol is to provide secure data communication with the goal of improving performance packet delay and routing efficiency for different attacks in MANET.

General Terms
MANET, Security

Keywords
AASR, Anonymous Routing, delay efficient routing

1. INTRODUCTION
Mobile Ad hoc Networks (MANETs) can be defined as autonomous system of mobile nodes connected via wireless links without using any existing network infrastructure. Each node acts as a host as well as a router and forwards each other's packets to enable the communication between nodes, not directly connected by wireless links. A central challenge in the design of ad hoc networks is the development of dynamic routing protocols that can efficiently find routes between the communicating nodes. The routing protocol must be able to keep up with the high degree of node mobility that often changes the network topology drastically and unpredictably. In adversarial network, it is difficult to provide trusted and secured communications. The nodes inside a network are not always trusted because a node within a network may become malicious. The adversaries outside a network may deduce the information about the communicating nodes or traffic flows by passive snooping. A secured routing protocol should be provided whenever nodes want to communicate with each other. End-to-end security mechanisms can provide some level of security for the data, valuable information such as identity and traffic of the communicating nodes may be easily determined from data analysis. An anonymous routing based technique should be modified to provide anonymity and to overcome attacks. Anonymity is a combination of unidentifiability and unlinkability. Unidentifiability indicates that the identities of the source and destination nodes should not be revealed to the other nodes in the network. Unlinkability indicates that the route and traffic flows between the nodes cannot be uncovered to the network [1].

2. RELATED WORK
Various methods to deal with the anonymity for MANETs have been proposed.

Trapdoor: A trapdoor is a common concept in cryptographic functions, which defines a one-way function between two sets. It is an information collection mechanism in which intermediate nodes add information elements, such as node IDs, into the trapdoor. Only the source and destination nodes can unlock and retrieve the elements using pre-established secret keys. The usage of trapdoor requires an anonymous end-to-end key agreement between the source and destination [2].

Onion Routing: It is a mechanism to provide private communications over a public network. The source node setup the core of an onion with a specific route message. During a route request phase, each forwarding node adds an encrypted layer to the route request message. The source and destination nodes do not necessarily know the ID of a forwarding node [3].

Group Signature: Group signature mechanism provides authentications without disturbing the anonymity. Every member in a group has a pair of group public and private keys issued by the group manager. The members generate its own signature by its own private key, and these signatures are verified by other members in the group without revealing the signer's identity [4].

J. Kong, X. Hong, and M. Gerla, in "ANODR: An identity-free and on-demand routing scheme against anonymity threats in mobile ad hoc networks" [6], proposed an on-demand protocol that works on the mechanism of broadcast and trapdoor information. The drawback of this approach is that every forwarding node in the path has to generate a fresh public/secret key pair for every RREQ message. These RREQs are flooded over the entire network, so every node needs to generate a fresh pair of key for every RREQ that is released in the network. The cost of generating key pairs increases due to overhead.

A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, in "An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks" [5], proposed a

protocol which permits only the reliable nodes to participate in transmission. The source node does not require gathering information about the topology of the network; it broadcasts the path disclosure message with some trust prerequisite, the intermediate nodes fulfilling the trust, embeds its ID and session key and encrypts the message. This message achieves the destination and it gets decrypted in each intermediate node and achieves the source. Source node obtains complete information about the intermediate nodes. Neighborhood nodes IDs are potentially uncovered. This protocol uses multicast mechanism and layered encryption. SDAR is not secured against Denial of Service attack. Messages are vast and rely on the quantity of bounces. This protocol restrains the efficiency.

R. Song, L. Korba, and G. Yee, in "AnonDSR: efficient anonymous source routing for mobile ad hoc networks" [7], presented a mechanism in which the anonymous route establishment relies upon the quantity of jumps between the source and the destination, time will be increased as number of hops increases, but it allows the destination nodes to know all the intermediate node IDs.

Y. Zhang, W. Lou, and Y. G. Fang, in "MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks" [8], proposed an algorithm to provide anonymity which depends on a unique sort of open key cryptosystem, the pairing-based cryptosystem, to accomplish unknown correspondence in MANET but it fails at the destination nodes because the destination node ID is present in every RREQ message in plain text.

L. Yang, M. Jakobsson, and S. Wetzel, in "Discount anonymous on demand routing for mobile ad hoc networks" [9], proposed the same system of ANODR at a lower cost. It has the advantage of accomplishing considerably lower computation and correspondence complexities at the cost of expense of a slight lessening of security insurances. Route requests in Discount-ANODR and in ANODR are parallel but the limitation is that intermediate nodes only know the destination of the request and the identity of the previous intermediate node but not the source node.

J. Paik, B. Kim, and D. Lee, in "A3RP: Anonymous and Authenticated Ad hoc Routing Protocol" [10], provides security to data packets by group signature but the A3RP used secure hash function to calculate the anonymous route using the real IDs of the destination node but it is not scalable as encrypted onion mechanism.

The existing protocols are vulnerable to the denial-of-service (DoS) attacks. The node IDs are exposed, which do not provide anonymity to the nodes in the adversarial network. Generating new pair of public/private key for each node makes the operation expensive. To overcome the problems associated with existing method recently AASR method was proposed by Wei Liu and Ming Yu, in "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments". In this paper author focused on the MANETs in adversarial environments, where the public and group key can be initially deployed in the mobile nodes. It was assumed that there is no online security or localization service available when the network is deployed. Therefore authenticated anonymous secure routing (AASR) is proposed to overcome the pre-mentioned problems. AASR method adopts a key-encrypted onion to record a discovered route and design an encrypted secret message to verify the RREQ-RREP linkage. Group signature is used to authenticate the RREQ packet per hop, to prevent intermediate nodes from modifying the routing packet. AASR is suffering from the worst delay performance and that is the main research problem.

3. PROPOSED METHOD

Here a new secure routing protocol called DEAASR is presented, which is based on existing AASR [1] with the goal of improving packet delay performance of AASR. At first, group and public key are initially deployed over mobile nodes in MANET. The AASR is implemented to overcome the existing problems. Then packet delay aware algorithm is implemented by modifying routing process of AASR to improve packet delay performance.

Algorithm 1: AASR
Step 1: Generate the PKI.
Step 2: PKI generation done by broadcasting source node ID.
Step 3: Extract the Public Key, Private Key and Session Key.
Step 4: Insert all three current keys into the routing table.
Step 5: At Source Node
Step 5.1: Extract the current routing information
Step 5.2: Get the current session key
Step 5.3: Generate the new session key and update the routing table entries
Step 5.4: Broadcast RREQ Packet
Step 5.5: Apply the Key encryption onion at intermediate nodes and destination node
Step 5.6: Signing by source node with its group private key
Step 5.7: Broadcasting finally the authenticated RREQ
Step 5.8: Set the status 'P' and update the routing table entry for current path with this status
Step 6: At Intermediate Node
Step 6.1: Verify the received packet with group private key
Step 6.2: If packet verification is successful then extract all details from the received packet else marked current received packet is from malicious node and drops it.
Step 6.3: Transfer the received packet further by following below steps of onion routing
Step 6.4: If the Nsq exists in the table but with an old timestamp, it has been processed before and will be ignored, else current rreq is new and it will be proceed further.
Step 6.5: Apply Decryption operation if its destination node, else forward it to next hope by performing the encryption operation by using the keys generated
Step 6.6: Signing the Source node with its group private key
Step 6.7: Set the status 'P' and updated routing table entry with current route
Step 7: At Destination node
Step 8: Step 6 are repeated to get the original data at original destination node.
Step 9: Stop

Delay Efficient Authenticated Anonymous Secure Routing (DEAASR) is concerned with optimizing and healing paths to reduce the number of hops and hence improving the routing performance packet delay.

On demand routing protocols maintain the routes those are currently active. A route is needed for message transfer so route discovery process is needed for data transfer. Most of the previously proposed routing protocols do not initiate a new path discovery process until there is a link failure. Because of movement of nodes in the network changes the shape of routing paths. This algorithm monitors the routing path and tries to shorten the length of path; which will increase the performance of AASR protocol. Each packet carries a "hop count (HC)" field in its header. HC is initialised

to zero at originating node and gets incremented by one at every hop of packet. Hop comparison array is maintained at each node of current communication path. Format of hop comparison array is <Src, Dest, HC, Neigh>, where Src is source address, Dest is destination address and Neigh is neighbour's address from which packet was broadcasted.

Consider source node Src_q and a destination node $Dest_q$. When node *a* receives a packet it first checks for the available shortest path. The algorithm is as follows.

Algorithm 2: Delay Aware Algorithm

Step 1: When node *a* receives or overhears a packet P, IF the node *a* is the final destination address, consume the packet. GOTO END;

Step 2: (Assume P belongs to <Src_q, $Dest_q$> flow). Compare <Src_q, $Dest_q$> to all the valid entries in the hop comparison array;

Step 3: IF there is no match with the entries, store <Src_q, $Dest_q$, HC_q, $Neigh_q$> in the hop comparison array;

Step 4: IF the packet is destined to *a* as the next-hop node,process the packet for forwarding further.

Step 5: (Assume that it matched with an entry <Src_q, $Dest_q$, HC_p, $Neigh_p$>) IF ($HC_q - HC_p > 2$), a short-cut is found, node *a* does the following:

Step 5.1: Send a message to $Neigh_p$ to update the routing table such that the next hop address for destination node $Dest_q$ is modified to the address of node *a*;

Step 5.2: Modify its routing table by making the next-hop address for destination $Dest_q$ as $Neigh_q$;

Step 5.3: Modify its hop comparison array, delete the entry corresponding to <Src_q, $Dest_q$>;

Step 6: Return the delay efficient path.

Step 7: Stop.

4. PERFORMANCE SIMULATION

Proposed protocol is implemented in NS-2 by extending AODV module.

4.1 Performance Metrics

- Throughput – Throughput is the percentage number of packets successfully reaching the destination over communication channel. It is measured in terms of bits per second.
- Packet Loss – It is the difference between number of packets sent or transmitted and number of packets received. Packet loss is proportional to packet drop. Lower value of packet loss means better the performance.
- Average End to End Delay – It is the average time taken by a data packet to arrive in the destination. Lower end to end delay means better performance of the protocol.

4.2 Results

Here two scenarios of simulation results are considered.

4.2.1 Scenario 1: Varying mobility speed

When mobility speed increases, the throughput varies. As compared to AODV and AASR, DEAASR achieves highest throughput. DEAASR achieves less packet loss ratio under different number of mobile scenarios as compared to AODV and AASR. Due to additional security processing time in RREQ flooding, AASR has longer delay than AODV. Since DEAASR uses path aware routing so its delay is lower than AASR.

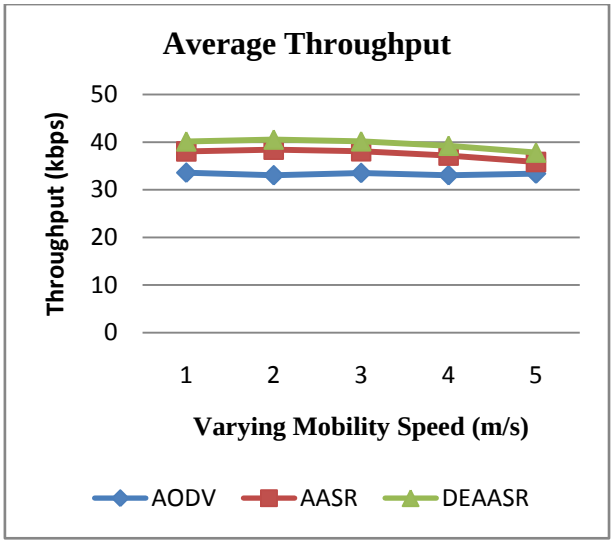

Fig 1: Throughput comparison under different mobility scenarios

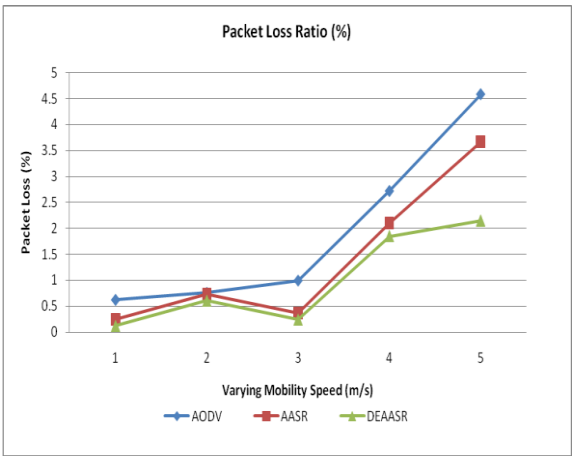

Fig 2: Packet Loss Ratio comparison under different mobility scenarios

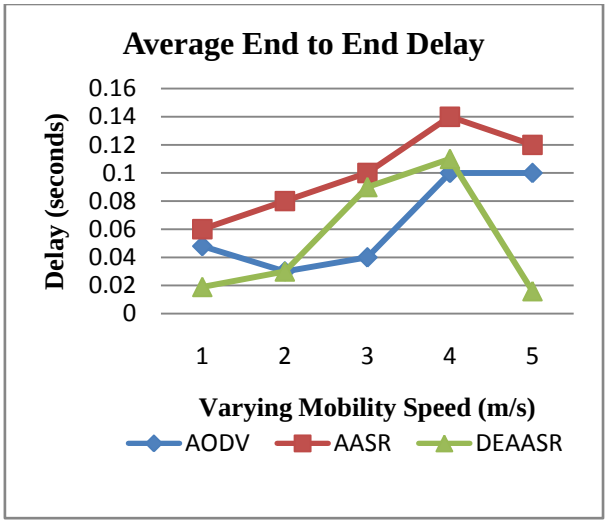

Fig 3: End to End Delay comparison under different mobility scenarios

4.2.1 Scenario 2: Varying number of malicious nodes

When number of malicious nodes increases, the average throughput of three protocols decreases. Since DEAASR has the ability to detect the packet dropping attack, it is better than AASR and AODV. DEAASR achieves less packet loss ratio as compared to AASR and AODV. AASR spends time in the security processing in the route discovery; their delays are higher than AODV. Since DEAASR uses path aware routing technique so its delay is lower than AASR.

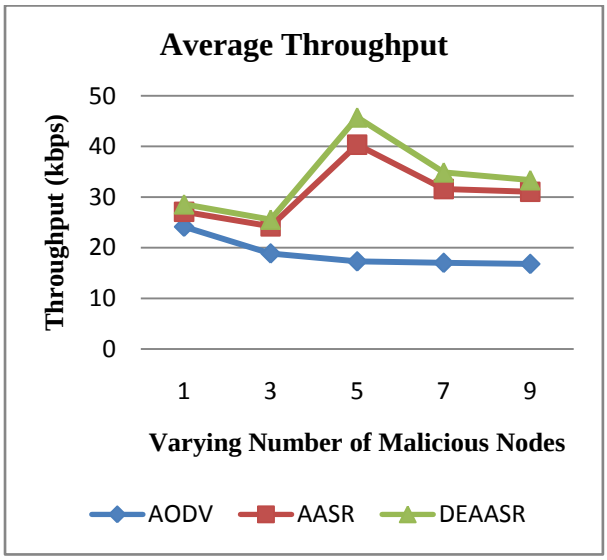

Fig 4: Throughput comparison under different number of malicious nodes

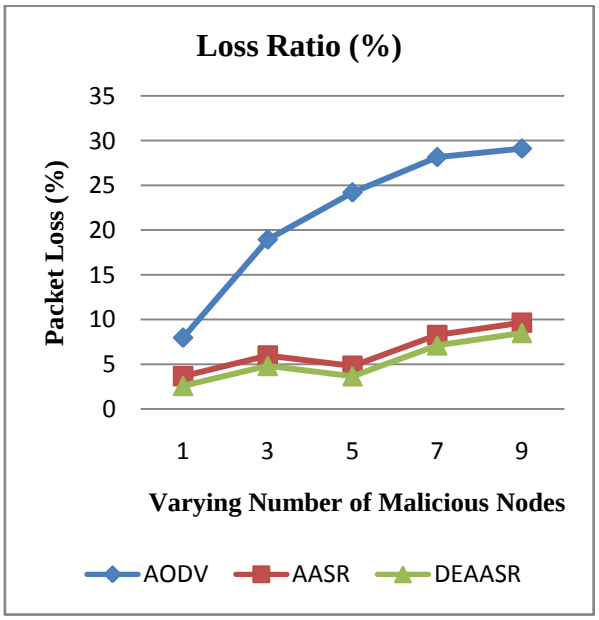

Fig 5: Packet Loss Ratio comparison under different number of malicious nodes

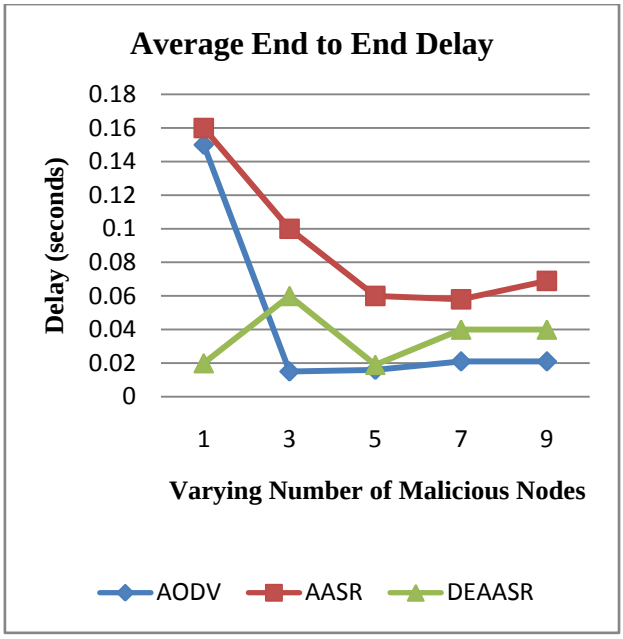

Fig 6: End to End Delay comparison under different number of malicious nodes

5. CONCLUSION

The DEAASR model is designed to provide anonymity. The group signature scheme prevents the active attacker without introducing the node identity. The onion routing scheme prevents the intermediate nodes from deducing the actual destination. DEAASR is compared with AODV and AASR, DEAASR provides higher throughput, reduced packet delay and lower packet loss ratio.

6. REFERENCES

[1] Wei Liu and Ming Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments" IEEE Transactions on VehicularTechnology,Volume:63, No:9,November 2014.

[2] S. William and W. Stallings, *Cryptography and Network Security, 4th Edition*. Pearson Education India, 2006.

[3] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous Connections and Onion Routing," *IEEE Journal on Selcted Area in Comm.*, vol. 16, no. 4, pp. 482–494, May 1998.

[4] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proc. Int. Cryptology Conf. (CRYPTO'04)*, Aug. 2004.

[5] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: a Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad hoc Networks," in Proc. IEEE Int'l Conf. Local Computer Networks (LCN'04), Nov. 2004, pp. 618–624.

[6] J. Kong, X. Hong, and M. Gerla, "ANODR: An identity-free and on-demand routing scheme against anonymity threats in mobile ad hoc networks," IEEE Trans. on Mobile Computing, vol. 6, no. 8, pp. 888–902, Aug. 2007.

[7] R. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymous dynamic source routing for mobile ad hoc networks," in Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN'05), Nov. 2005.

[8] Y. Zhang, W. Liu, W. Lou, and Y. G. Fang, "MASK: Anonymous On-Demand Routing in Mobile Ad hoc Networks," IEEE Trans. on Wireless Comms., vol. 5, no. 9, pp. 2376–2386, Sept. 2006.

[9] L. Yang, M. Jakobsson, and S. Wetzel, "Discount anonymous on demand routing for mobile ad hoc networks", in *Proc. Int. Conf. SECURECOMM*, pp. 1–10, Aug. 2006.

[10] J. Paik, B. Kim, and D. Lee, "A3RP: Anonymous and Authenticated Ad hoc Routing protocol," in Proc. International Conf. on Information Security and Assurance (ISA'08), Apr. 2008.

[11] C. Perkins, E. Belding-Royer, S. Das, *et al.*, "RFC 3561 - Ad hoc On-Demand Distance Vector (AODV) Routing," *Internet RFCs*, 2003.