Implementation and Analysis of Dynamically Randomize-Anonymous Location-Based Efficient Routing Protocols for MANET's

G. Priyanga Ancy
PG Student, Dept. of ECE, Periyar Maniammai University
Thanjavur, Tamilnadu, India

C. Narmadha
Assistant Professor [SS], Dept. of ECE, Periyar Maniammai University
Thanjavur, Tamilnadu, India

Abstract— Mobile ad hoc network (MANET) is a self-routing, infrastructure less network of mobile nodes are communicated with wireless standard to exchange required data. MANETs uses anonymous routing protocol for increase security performance, hides nodes unique individuality from outsider therefore observer cannot attack the security of the network. Existing routing protocols are relying on hop-by-hop encryption and redundant traffic. However they are having high cost and provide low secrecy protection for sources, destination, and route anonymity. Also it is frequently choosing the routing path. Hence to provide high secrecy protection (for sources, destination, and route) with low cost; we propose a Dynamically Randomize-Anonymous Location-based Efficient Routing protocol (DR-ALERT). DR-ALERT is taken two phases: key update process (source node to certificate authority) and key renewal process (certificate authority to destination node). Phase 1: Dynamically a partition the network field into number of zones using ALERT protocol and GPSR is randomly chooses a high level of energy nodes in zones. Named as intermediate Relay nodes also it is form a non-traceable anonymous route. Still source node updated encrypted key to the Relay node and it is authorized then it is given the required data packets to the relay nodes. However this same process is forward to last k-node and k-node then forward to certificate authority. In a longest distance routing path it will forward the data packets using Random forwarder. Phase 2: Certificate authority in a cluster wants to communicate with destination node in some other cluster; it randomly sends the Renewal key + Data packet to the Border Node using RICR protocol. Border Node will check destination node is in its own cluster, it will (In a long distance it will use the Random forwarder) forward the packet to the destination node through the shortest path. Experimental results and theoretical analysis of our proposed DR-ALERT is achieves better route anonymity protection with lower cost compared to Existing anonymous routing protocols.

Keywords— MANET, DR-ALERT, GPSR, RICR, Key Update Process, Key Renewal Process, Relay Node, Random Forwarder, Certificate Authority.

I. INTRODUCTION

MANET stands for mobile ad-hoc network is a very fast development and advancement in the field of mobile computation and used group of wireless of mobile nodes. Mobile nodes or devices (mobiles, laptops and sensors) are communicated with each other wireless standard and to exchange the required data packets without know their geographical position and physical substructure [10]. Characteristics of MANETs such as distributed procedure, multi hop routing, dynamic topology, light weight of terminals and shared physical standard [2]. The advantages of MANETs are climbable accommodates the adding of more nodes, improved flexibility, strong due to decentralize organization and the network should be group at any place and time [13]. Challenges in MANETs such as small amount of bandwidth, packet losses owing to transmission mistakes, hidden deadly problem, unnecessary of routing overhead, battery limitations. The wireless applications of MANETs are Military, Education, Commerce, and Entertainment [16]. But the other belvedere of security of MANET, these networks gets easily broken their security performance. Therefore mostly the security issues are data lost and analysing data and traffic eavesdropping method or attacking routing protocol. Also security is attacked by security attacker is mainly classified into two types Passive attack and Active attack [8]. Overcome this security issue one of the most important solution is to use anonymous routing protocol in the network field that cannot be identified by every other nodes or attacker or observer. Anonymous routing protocol for increase security performance, hides nodes unique individuality from

http://dx.doi.org/10.21172/1.71.006

outsider therefore observer cannot attack the security of the network [3]. Existing routing protocols are relying on hop-by-hop encryption and redundant traffic. However they are having high cost and provide low secrecy protection for sources, destination, and route anonymity. Also it is frequently choosing the routing path.
Anonymity routing protocols in MANETs is can be mainly divided into two types: 1) Proactive DSDV [9], ALARM [11] and 2) Reactive protocols AAD [1], AO2P [19]. Existing Routing protocols are further mainly classified into two categories such as hop-by-hop encryption [5], [7], [15], [19], [20], [21] and redundant traffic [9], [11].

In this paper, we propose a Dynamically Randomize-Anonymous Location-based Efficient Routing protocol (DR-ALERT) is to support key update and key renewal process methods. This proposed method overcomes the existing limitation such as speed, threshold and energy consumption of MANET's. We use the software for Network Simulator version is 2 (NS2) to implement and analysis the proposed method. Section II defines the background information about the Existing anonymity routing protocols. Section III discuss about the new proposed method. Finally simulation and results are discussed in Section IV.

II. RELATED WORKS

In this section, we discuss about the background information of the Existing anonymity routing protocols. MANET's uses anonymous routing protocol for increase security performance [18]. Hence hides nodes unique individuality from outsider therefore observer cannot attack the security of the network. Anonymity routing protocols in MANETs is can be mainly divided into two types: Proactive and Reactive protocols [4]. Proactive protocols are maintains one or more routing tables [14]. Therefore address of nodes is transmitting hello messages periodically to update routing tables. Also it is called for table driven routing protocol. Its route discovery is fast and packet delivery of reliability is good. But it is need large routing overhead and wants broken hello message to find routing variations. Distance vector (DV) protocol [12], Destination Sequenced Distance Vector (DSDV) protocol [9] are the examples of proactive protocols. Reactive protocols are does not have any pre-determined routing tables. Also it is called for on demand routing protocol or source initiated. Source node it wants to send packets to its destination it will initiates a route discovery process all over the network. Hence route discovery process is complete by way of using flooding of route request data packets. It needs less routing overhead and it consume fewer resources owing to the nonattendance of large routing tables. But its route finding time is high inactivity and unnecessary flooding is can lead to network blockage. Dynamic Source Routing (DSR) [6] and Ad-hoc On Demand Routing (AODV) [15] are the examples of reactive protocols. Existing anonymity routing protocols are further more mainly classified into two categories such as hop-by-hop encryption and redundant traffic. These existing methods are to increase the security levels. Hop-by-hop encryption is more classified into two types' hop-by-hop authentication and onion routing. **1) Hop-by-hop Encryption:** A packet is encrypted in the transmission of two nodes in route, avoiding attacker to identify the communicating of two nodes. Hop-by-hop Encryption is divided into two types Onion routing and Hop-by-hop authentication. **Onion routing** is consists the source node of data packets are encrypted and decrypted layer by layer each and every another nodes (i.e., hop by hop) along the routing path. Onion routing is also strengthening source, destination and route anonymity production [20], [21]. **Hop-by-hop authentication** is used to avoid observer after contributing in the routing path toward confirm route anonymity. It is also strengthening production in source anonymity but weakest production in destination and route anonymity [5], [19], [7]. Disadvantage is high cost as a result of the use of hop-by-hop public-key cryptography or complex symmetric key cryptography. **2) Redundant traffic:** Redundant traffic-based routing protocols are uses redundant traffic for example multicast, local broadcasting, and flooding and also to clear doubtful possible attackers. Redundant traffic based routing protocols are commonly Strengthen Source anonymity production but weaken destination and route anonymity production [9], [11]. Disadvantage is very high overhead experienced through the redundant operations or packets and most important to high cost.

Greedy and Perimeter forwarding algorithm is Hop-by-hop authentication and it is a reactive type protocol this is proposed by Brad Karp and H. T. Kung [5]. It used for finding the positions of routers and packet forwarding decisions. Each node location information is encrypt and transmitted to the location server. Greedy forwarding algorithm is to forward data packets to nodes that are continuously ever closer to the destination. But particular regions of the network where such a greedy path does not be real. Therefore recovers by forwarding in perimeter mode now packets pass through successively reaching a node closer to the destination and where greedy forwarding starts again. Strengthen in source and destination anonymity production but weakest in route anonymity production. Wu et al. proposed an Ad Hoc On-demand Position-based Private Routing Protocol (AO2P), Hop-by-hop authentication and it is a reactive type protocol [19]. A node chooses the neighbor that can reduce the highest distance from the destination. Strengthen in source anonymity production and weakest in destination and route anonymity production. Defrawy et al. Proposed Privacy-Friendly Routing in Suspicious MANETs (PRISM) is used on- location basis method [7]. Also Hop-by-hop authentication and it is a reactive type protocol. Then long-term node identifiers or public keys of any information is does not assumed. Strengthen in source and destination anonymity production but weakest route anonymity production. Perkins et al. proposed Ad- Hoc On-Demand Distance Vector (AODV), both unicast and multicast routing and it is a reactive type protocol [15]. Two important functions are first one is route finding and second one is route maintenance. It minimizes the number of required broadcasts but it taken high time in route finding.

Zhang et al. Proposed by Anonymous on Demand Routing Protocol (ANODR), onion routing and it is a reactive type protocol [21]. Trapdoor Boomerang Onion (TBO) function is used as a replacement for public key-based encryption. Strengthen in source, destination and route anonymity production. But it needs onion construction in both find routing and return routing. So overcome this problem Yang et al. introduced by Discount-Anonymous on Demand Routing Protocol (Discount-ANODR) [20]. Also onion routing and it is a reactive type protocol. Therefore it constructs onions routing only on the return routes. Strengthen in source, destination and route anonymity production. Aad et al. proposed by Anonymous in Ad hoc Networks (AAD), Combines Hop-by-hop encryption (onion routing) and Redundant traffic (multicast) and it is a reactive type protocol [1]. It uses packet coding policies to constantly change the packets. Strengthen in both destination and route anonymity production but weaken in source anonymity production.

Guoyou He proposed by Destination Sequence Distance Vector (DSDV), redundant traffic and it is a proactive type protocol [9]. Each node maintains routing tables or table driven with destination address hope count and sequence number. Avoid looping but very high overhead and lower reliability of data delivery. Karim El Defrawy et al. proposed by Anonymous Location-Aided Routing in Suspicious MANET (ALARM), redundant traffic and it is a proactive type protocol [11]. Each nodes communications its location data to its authenticated neighbor nodes and later anonymous route discovery each node should be build a map. Strengthen in Source anonymity production but weaken in destination and route anonymity production. Sasikumar and Anitha proposed by Cluster Based Routing Protocol (CBRP) [17]. It based on Inter-cluster and Intra cluster routing algorithm which offers minimum cost communication between clusters.

III. PROPOSED METHOD

Anonymous routing protocol for increase security performance, hides nodes unique individuality from outsider therefore observer cannot attack the security of the network. Existing routing protocols are relying on hop-by-hop encryption and redundant traffic. However they are having high cost and provide low secrecy protection for sources, destination, and route anonymity. Also it is frequently choosing the routing path. Hence to provide high secrecy protection for sources, destination, and route with low cost. In this paper we propose a Dynamically Randomise-Anonymous Location-based Efficient Routing protocol (DR-ALERT). DR-ALERT is used for hierarchical zone partition process, zone partitioning consecutively splits the smallest zones. DR-ALERT is taken two phases: key update process and key renewal process. Key update process for source node to certificate authority and key renewal process for certificate authority to destination node.

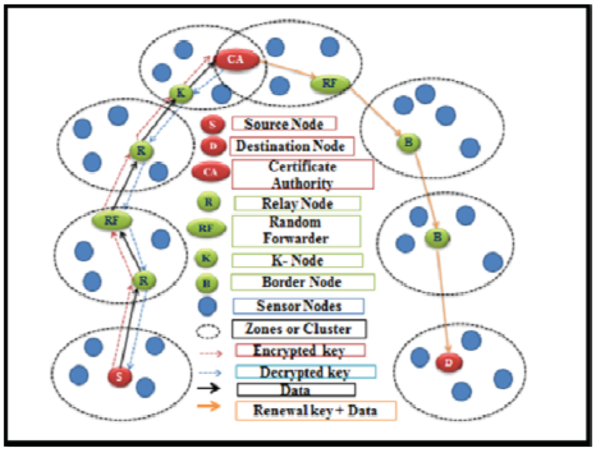

Figure 1: Proposed Scheme Structure

1. Phase 1: Key update process

Key update process for source node to certificate authority. Dynamically a partition the network field into number of zones using ALERT protocol and each routing step, a source partitions the network field in order to separate itself. It then used Greedy Perimeter Stateless Routing (GPSR) algorithm randomly chooses a high level of energy nodes in the other zone named as intermediate relay node and to send the data to the relay node. Also relay nodes are forming a non-traceable anonymous route. Still source node updated encrypted key to the Relay node and it is authorised then it is given the required data packets to the relay nodes. However this same process is forward to k-node in the Certificate Authority (CA) zone, providing k-anonymity to the CA. Where k is a predefined integer. K is used to control the degree of anonymity protection for the CA. Then k-node to forward that same process to CA. In a longest distance routing path it will forward the data packets using Random forwarder.

2. Phase 2: Key renewal process

Key renewal process for certificate authority to destination node. Certificate authority in a cluster wants to communicate with destination node in some other cluster using Least Significant Rotate algorithm. Then it is randomly sends the Renewal key + Data packet to the Border Node using Random Inter Cluster routing protocol (RICR). Border Node will check destination node is in its own cluster and if it is present it will forward the packet to the destination node through the shortest path. In a long distance it will use the Random forwarder to use forward the data. Uncertainty the node is not present in its cluster and it transmissions the packet to another clusters border node. This same process is repeated check-out the packet reaches to the correct destination node. After the delivery of packets, the destination sends a confirmation to the source node. If the source has not received the confirmation during a predefined time period, it will resend the packets.

3. Algorithm

STEP1: The first step in the proposed DR-ALERT system to taken key update process for in source node to CA. A source partitions the network field in order to separate itself. We take up source destination and node randomly in the different time intervals.

STEP2: GPSR a novel routing protocol for wireless datagram networks that uses the positions of routers and a packet's destination to make packet forwarding decisions. It used for finding the positions of routers and packet forwarding decisions. Each node location information is encrypt and transmitted to the location server. Greedy forwarding algorithm is to forward data packets to nodes that are continuously ever closer to the CA. But particular regions of the network where such a greedy path does not be real. Therefore recovers by forwarding in perimeter mode now packets pass through successively reaching a node closer to the certificate authority and where greedy forwarding starts again.

STEP3: GPSR algorithm randomly chooses a high level of energy nodes in the other zone named as intermediate relay node and to send the data to the relay node. Still source node to send encrypted key to the Relay node.

Encrypted function is taken for DES (Data Encryption Standard) algorithm. In a longest distance routing path it will forward the data packets using Random forwarder.

STEP4: After the getting of encrypted key the relay node to give the decrypted key to source node and it is authorized then it is given the required data packets to the relay nodes. Decrypted function is taken for Compliment Function algorithm. Repeat the step until to reach k node. K nodes where CA resides the destination zone. Then k-node to forward that same process to CA.

STEP5: The next step key renewal process for certificate authority to destination node. Renewal key process are using LSB (Least Significant Bit Rotation algorithm) algorithm. Certificate authority in a cluster wants to communicate with destination node in some other cluster using RICR protocol; it randomly sends the Renewal key + Data packet to the Border Node.

STEP6: Border Node will check destination node is in its own cluster and if it is present it will forward the packet to the destination node through the shortest path. When in a long distance it will use the Random forwarder to use forward the data.

STEP7: Uncertainty the node is not present in its cluster and it transmissions the packet to another clusters border node. This same process is repeated check-out the packet reaches to the correct destination node.

STEP8: After the delivery of packets, the destination sends a confirmation to the source node. If the source has not received the confirmation during a predefined time period, it will resend the packets.

IV. RESULTS AND DISCUSSION

We use Network simulator (NS2) to show the performance of our proposed scheme. A MANETs consists of 40 sensor nodes are randomly deployed over region of 1000 ×1000 m^2 used in this simulation. The size of the data packet is 50 bytes. Destination-Sequenced Distance-Vector Routing Protocol (DSDV) is used. We have 8 cluster groups. As compared to existing scheme, our proposed scheme has better performance in terms of Speed, Packet Delivery rate, and Throughput. The following section shows the simulation parameters, results and comparison performance of the proposed system. Table 1 shows the simulation parameters for the proposed method.

1. Simulation Parameters

Parameter	**value**
Field size	1000×1000 m^2
Number of sensor nodes	40
Propagation type	Two ray ground
Routing type	DSDV
Packet size	50bytes
Channel	Wireless
Simulation time	80 seconds

Table 1 Simulation Parameters

2. Performance Results

In this section, the performance of our protocol is compared with the existing method in terms of Speed, Throughput and Packet Delivery rate.

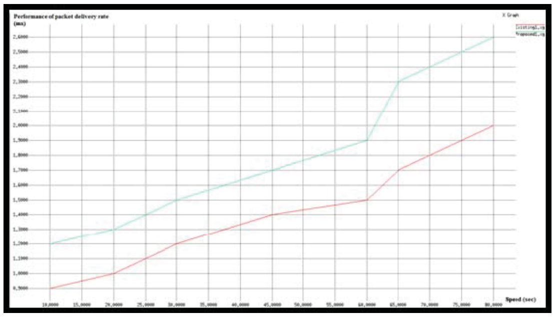

Fig. 2 Performance of Packet Delivery rate Vs Speed

Figure 2 shows the comparison of existing and proposed anonymous routing protocol methods in terms of Packet Delivery rate and Speed. In this figure, the performance of proposed routing protocol is good packet delivery rate level as compared to existing routing protocol.

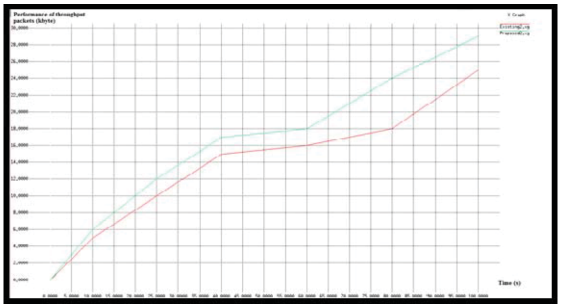

Fig. 3 Performance of Throughput packets Vs Time

Figure 3 shows the comparison of existing and proposed anonymous routing protocol in terms of Throughput. In this figure, the performance of proposed routing protocol is good throughput level as compared to existing routing protocol.

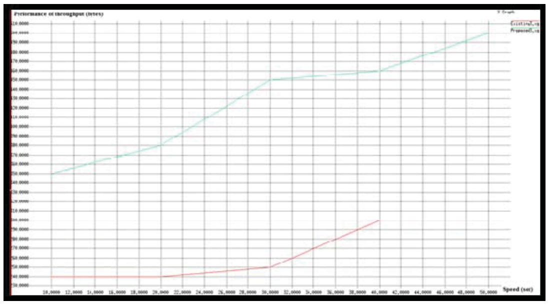

Fig. 4 Performance of Throughput Vs Speed

Figure 4 shows the comparison of existing and proposed anonymous routing protocol in terms of Throughput and Speed. In this figure, the performance of proposed routing protocol is good throughput and speed level as compared to existing routing protocol.

V. CONCLUSION

Previous year there are number of routing protocols are available for MANET's for sharing the information between source and destination securely. Existing routing protocols are relying on hop-by-hop encryption and redundant traffic. Although sharing information between source and destination and the security to source, destination along with routers is need to avoid the gain access from the unauthorized user. The some existing protocols provide protection only of source and destination locations or only to route locations. However they are having high cost and provide low secrecy protection for sources, destination, and route anonymity. Also it is frequently choosing the routing path. Hence to provide high secrecy protection (for sources, destination, and route) with low cost; we propose a Dynamically Randomize-Anonymous Location-based Efficient Routing protocol (DR-ALERT). DR-ALERT is taken two phases: key update process (source node to certificate authority) and key renewal process (certificate authority to destination node). Our proposed protocol offers security in terms of location and identity anonymity for source, destination as well as routes. Since DR-ALERT uses dynamic partition and random selection of nodes it founds a dynamic routing path for different packet transmissions. Also it should be reach comparable routing efficiency to the base-line of GPSR algorithm. Experimental results and theoretical analysis of our proposed DR-ALERT is achieves better route anonymity protection with lower cost compared to Existing anonymous routing protocols.

REFERENCES

[1] Aad I., Castelluccia C., and Hubaux J., “Packet Coding for Strong Anonymity in Ad Hoc Networks,” Proc. Securecomm and Workshops, 2006.

[2] Aarti and Dr. Tyagi S. S., “Study of MANET: Characteristics, Challenges, Application and Security Attacks”, Volume 3, Issue 5, May 2013 ISSN: 2277 128X, Department Computer Science and Software Engineering, MRIU Faridabad, Haryana, India.

[3] Anupriya Augustine and Jubin Sebastian E., “A Comparative Study of Efficient Anonymous Routing Protocols in MANET”, IJRET: International Journal of Research in Engineering and Technology EISSN: 2319-1163 | PISSN: 2321-7308.

[4] Basu Dev Shivahare1 , Charu Wahi2 and 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, Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 3, March 2012).

[5] Brad Karp and Kung H. T., “GPSR: Greedy Perimeter Stateless Routing for Wireless Networks”, Harvard University / ACIRI, karp@eecs.harvard.edu, MobiCom 2000.

[6] David B., Johnson David A., and Maltz Josh Broch, “DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks”, 2008.

[7] Defrawy K.E., and Tsudik G., “PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs),” Proc. IEEE Int’l Conf. Network Protocols (ICNP), 2008.

[8] Gagandeep, Aashima and Pawan Kumar, “Analysis of Different Security Attacks in MANETs on Protocol Stack”, International Journal of Engineering and Advanced Technology (IJEAT), Volume-1, Issue-5, June 2012.

[9] Guoyou He, “Destination-Sequenced Distance Vector (DSDV) Protocol”, Networking Laboratory, Helsinki University of Technology, ghe@cc.hut.fi, 2002.

[10] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, “An Overview of Mobile Ad Hoc Networks: Applications and Challenges”, Department of Information Technology (INTEC), Ghent University – IMEC vzw, Sint Pietersnieuwstraat 41, B-9000 Ghent, Belgium, Session 4.

[11] Karim El Defrawy, and Gene Tsudik, “ALARM: Anonymous Location-Aided Routing in Suspicious MANETs”, IEEE Transactions On Mobile Computing, Vol. 10, No. 9, September 2011.

[12] Malin Bornhager, “Distance Vector Routing Protocols”, Halmstad University, Version 2002-1.

[13] Mohit Kumar and Rashmi Mishra, “An Overview of MANET: History, Challenges and Applications”, Indian Journal of Computer Science and Engineering (IJCSE), Vol. 3 No. 1 Feb-Mar 2012.

[14] Mohseni S., Hassan R., Patel A., Razali R., “Comparative review study of reactive and proactive routing protocols in MANETs”, 4th IEEE International Conference on Digital Ecosystems and Technologies, 304-309, 2010.

[15] Perkins C., Belding-Royer E., and Das S., “Ad-Hoc on-Demand Distance Vector (AODV) Routing”, RFC3561, July 003.

[16] Priyanka Goyal, Vinti Parmar and Rahul Rishi, “MANET: Vulnerabilities, Challenges, Attacks, Application”, IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[17] Sasikumar M., and Dr. Anitha R., “Cluster Based Routing Protocol for Wireless Sensor Networks”, International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1 Issue 9 (October 2014).

[18] Sunil Taneja and Ashwani Kush, “A Survey of Routing Protocols in Mobile Ad-Hoc Networks”, International Journal of Innovation, Management and Technology, Vol. 1, No. 3, 279-285, August 2010.

[19] Wu X.X., and Bhargava B., “AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol,” IEEE Transactions on Mobile Computing, vol. 4, no. 4, pp. 335-348, July 2005.

[20] Yang L., Jacobson M., and Wetzel S., “Discount Anonymous On Demand Routing for Mobile Ad Hoc Networks,” SECURECOMM, vol. 6, 2006.

[21] Zhang Y., Liu W., Lou W., and Fang Y., “MASK: Anonymous On demand Routing in Mobile Ad Hoc Networks,” IEEE Transactions on Wireless Communications, no. 9, 2006.