International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Location Aware Cluster Based Secured Anonymous Routing for Manet

Nandini S. Patil[1], Rekha Patil[2]

[1]M.Tech, Department of Computer Science and Engineering,
Poojya Doddappa Appa College of Engineering, Gulbarga, Karnataka, India

[2]Associate Professor and HOD, Department of Computer Science and Engineering,
Poojya Doddappa Appa College of Engineering, Gulbarga, Karnataka, India

Abstract: ***A MANET is a type of Ad-Hoc network that can change locations and configure itself on the fly. The Ad-hoc On Demand Distance Vector (AODV) protocol used for stable route which incorporates nodes with least relative mobility between them and the Public Key Cryptographic method for secured transmission which is used for message authenticity is proposed .The Cluster heads initiate the key generation ,keys are distributed from the cluster heads which reduces the overall overhead of the network .The effects of using different transmit powers on the average power consumption and end-to-end network throughput in a wireless ad-hoc environments investigated which helps in reducing the system power consumption, pro-longing the battery life of mobile nodes and improves end-to-end network throughput due to minimizing interference ranges, reduction in the average number of hops to reach a destination ,the probability of having isolated clusters ,and the average number of transmissions .The protocol dynamically determine an optimal connectivity range by adapting their transmit powers so as to only reach a subset of the nodes in the network. The connectivity range would then be dynamically changed in a distributed manner so as to achieve the near optimal throughput. The work is simulated using Omnet++ 3.3.The simulation results are presented showing that the proposed increases packet delivery ratio, throughput .It also reduces the latency and energy consumption.***

Keywords: AODV, Public Key Cryptographic, MANET.

1. Introduction

A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Each device in MANET is free to move independently in any direction, and will change its links to other devices frequently. Each must forward traffic unrelated to its own use, therefore be a router. The challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. Mobile ad hoc network is a challenging research area because of its dynamic topology, power constraints, limited range of each mobile host's wireless transmissions and security issues etc. Stand-alone MANET, it has limited applications, because the connectivity is limited to itself. MANET user can have better utilization of network resources only when it is connected to the Internet. Global connectivity adds new security threats to the existing attacks on MANET. In a dynamic environment like MANET where node configuration changes frequently, assuring a secured routing is difficult. If the nodes are highly mobile, the route stability suffers. Mobile Adhoc network is an autonomous network of mobile nodes where the mobiles use the services of other mobiles for routing and packet transmission. Due to decentralized nature of the network such a security system requires frequent encryption and decryption, no control over the sessions due to decentralized topology, no power control technique due to non centralized architecture. Frequent mobility requires frequent route discovery. Data Transmission is not safe hence Security introduces lot of energy loss which is guaranteed by adopting secured public key cryptography for MANET. The objective is to propose a location aware routing cluster based routing on relative derivative of speed and direction of movement. We further propose public key cryptography based secured routing. In this paper we propose a combination of the cluster based routing with Position aware routing and secure the data transmission using RSA technique to derive a new routing and transmission protocol for Manet to improve the performance of system. The Cluster heads initiate the key generation, keys are distributed from the cluster heads, load is distributed through cluster heads which are essentially more energy efficient nodes. This approach can significantly decrease the energy consumption so as to reduce the routing overhead, and can also improve the routing performance. The Public Key Cryptographic ensures that keys are encrypted and decrypted the intruder guessing. Further it limits the necessity of key exchange rate that can dissipate huge node energy.

2. Organization

This paper is organized as follows, section 3 describes related work. Section 4 details the system design and implementation. Section 5 presents the performance evaluations of our system design. Finally, section 6 presents some concluding remark.

3. Related Work

A mobile ad hoc network is a self-configuring infrastructure less network of mobile devices connected by wireless. Each

device in MANET is free to move independently in any direction and change its links to other devices frequently. [1] Geographic Adhoc routing preserve location privacy, proposes an anonymous geographic routing algorithm, present's superiority in scalability.[2] Proposes novel packet coding techniques that make the combination of multicast or on onion routing to thwart global attackers or local attackers ,integrating the advantages in more complete and robust solution. [3] Proposes prevention attacks against routing in ad hoc networks ,design and performance evaluation of a new secure on-demand ad hoc network routing protocol.[4] propose the anonymous secure routing protocol that provide additional properties on anonymity ,ensure the security against attacks.[5] Defines GHT for the application workloads as analytically predict, offers high data availability, and scales to large sensor net deployments ,even when nodes fail or are mobile.[6] Reference Point Group Mobility(RPGM) is introduced, it investigate the impact of the mobility model on the performance of a specific network protocol or application.[7] proposes GLS which is a new distributed location service which tracks mobile node locations.[8] An anonymous on-demand routing protocol for mobile ad hoc networks is proposed for deployed in hostile environments addressing two related problems, route anonymity and location privacy.[9] propose a novel technique to address the anonymity problem at a lower cost which is dub Discount-ANODR ,which achieves lower computation and communication complexities at the cost of a slight reduction of privacy guarantees.[10] Secure Efficient Ad hoc Distance vector routing protocol (SEAD) is designed based on the design of the Destination-Sequenced Distance-Vector routing protocol (DSDV),performs well over the range of scenarios and is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of any active attackers or compromised nodes in the network.

4. Methodology

Manet algorithms mainly focus on establishing routes, and maintaining these routes under frequent and unpredictable connectivity changes. The implicit assumption in most of the earlier work is that nodes are not aware of each other's location and relies on hop based routing. In a dynamic environment like MANET where node configuration changes frequently, assuring secured routing is difficult. The advantage of this approach is reaching a large number of nodes in a single hop and almost all of the nodes in the network in two hops. The price paid is twofold, namely high power consumption and higher interference, which results in a large number of collisions. If the link cost is taken to be the transmitted power, it is straightforward to notice that the Cost of the Links is equal to Pmax. Hence objective of the work is to propose a location aware routing based on relative derivative of speed and direction of movement. We further propose public key cryptography based secured routing.

4.1. Message Transmission

Each mobile node has a direct link to the closest N out of (n-1) mobile nodes. We call these N nodes a cluster. Given, the mobile node adjusts its power to reach at most the farthest node within its cluster. We assume that there is no power adaptation within the cluster. The lower power consumption and possibly, a node's transmission will cause lower interference to other simultaneous transmissions, when compared to the previous cases. The protocols would first dynamically determine an optimal connectivity range wherein they adapt their transmit powers so as to only reach a subset of the nodes in the network.

The connectivity range would then be dynamically changed in a distributed manner so as to achieve the near optimal throughput. Minimal power routing is used to further enhance performance. The improvement is in achieving tradeoffs between minimizing interference ranges, reduction in the average number of hops to reach a destination, the probability of having isolated clusters, and the average number of transmissions (including retransmissions due to collisions).Data transmission is protected by introducing secured public key cryptography. Keys are distributed from the cluster heads which reduces the overall overhead of the network.

4.2. Cluster Head Communication

For communications, the algorithms generates to each cluster head a public key to encrypt the data packet with individual keys (a computation cost proportional to cluster size)which is decrypted using private key by other cluster heads, reduces the overall overhead of the network, communication cost, lower power consumption, lower interference to transmissions. The connectivity range would then be dynamically changed in a distributed manner to achieve the near optimal throughput.

4.3. Authentication

Authenticity means that when a user receives a message, it is assured about the identity of the sender. The authenticity requirement can be translated in the context of secure multicast into two requirements on key and data distribution.
Data authenticity: The cluster head can distinguish among the data sent by the another cluster head and the malicious data sent by an attacker.

4.4. Algorithm

Step 1: Cluster formation using

- Degree of connectivity range
- Energy

n handle Hello method whenever a hello Packet Comes Energy will be retrieved from physical layer.

Step 2: Cluster Head Calculation Degree of Neighborhood should be high Entropy, Low, low Mobility.

Step 3: Makes use of Public Key Cryptographic method for generating keys for security

Table 1: Key Generation.

Key Generation	
Select p, q	p, q both prime, p≠q
Calculate n = p×q	
Calculate $\phi(n) = (p-1)\times(q-1)$	
Select integer e	$gcd(\phi(n),e) = 1;\ 1<e<\phi(n)$
Calculate d	
Public key	KU = {e, n}
Private key	KR = {d, n}
Encryption	
Plaintext:	M < n
Ciphertext:	$C = M^e \pmod n$
Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Cluster head initiates encryption which is done using the public key component e and the modulus n.Obtain the recipient's public key (n,e),represent the plaintext message as a positive integer m < n,compute the cipher text c = $m^{\wedge e}$ mod n, Send the cipher text c to the recipient. Other cluster heads that come in the route of data transmission decrypts using private key is similar to the encryption except that the keys used are different, recipient uses his private key (n,d) to compute m = $c^{\wedge d}$ mod n,extract the plaintext from the integer representative m.

Step 4: End.

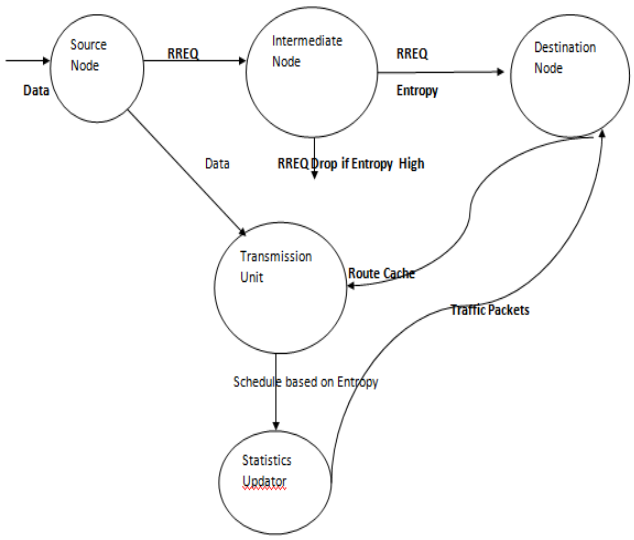

Figure 1: Data Flow Diagram

5. Results

5.1. Simulation Parameters

Table 2: Simulation Parameters

Parameters	*Value*
Simulator	OMNET 4.2
Application Rate	1000
Number of nodes	30
Pause Time	118s
Packet Size	512bytes
Mobile Host Max Speed	20
Threshold	2

In the fig 2, as the number of nodes increases, packet delivery ratio remains consistent at application layer.Hence by comparing the graphs of present with proposed system, present is more efficient in delivering packet.

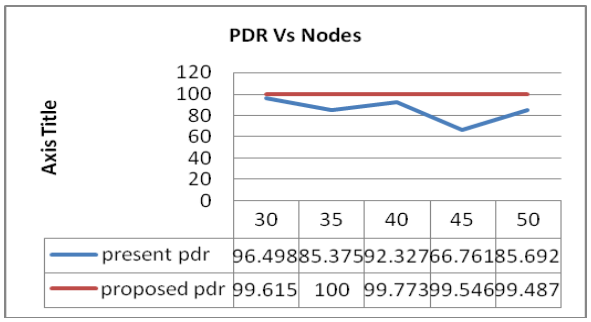

Figure 2: Packet delivery ratio Vs Number of Nodes.

In the fig 3, as the number of nodes increases, the latency decreases. This is due to advantage of cluster head formation, later latency reaches the constant level. Hence by comparing the graphs of present with proposed system, present is more efficient in decreasing the latency.

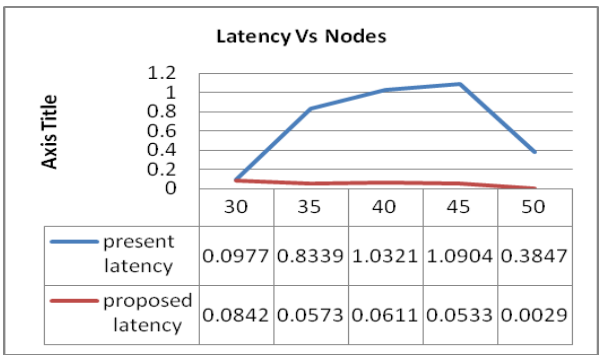

Figure 3: Latency Vs Number of Node

In the fig 4, as the application rate increases, the average cluster lifetime decreases .The comparison graph shows that proposed system average cluster lifetime is much more better than the present system.

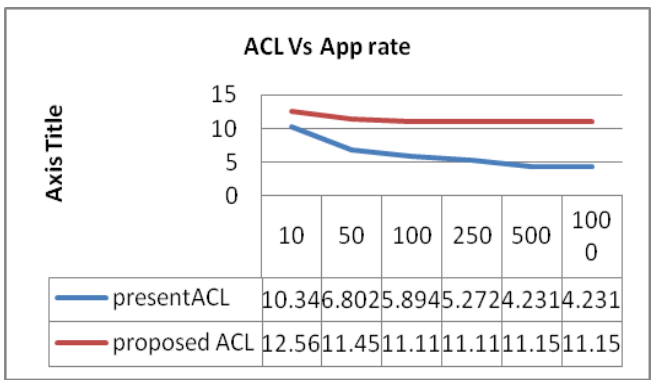

Figure 4: Average Cluster Lifetime Vs Application Rate

In the fig 5,as the number of nodes increases,throughput increases due to congestion in the network but the processing of packets will drop when node number increase to 45 in the proposed work.

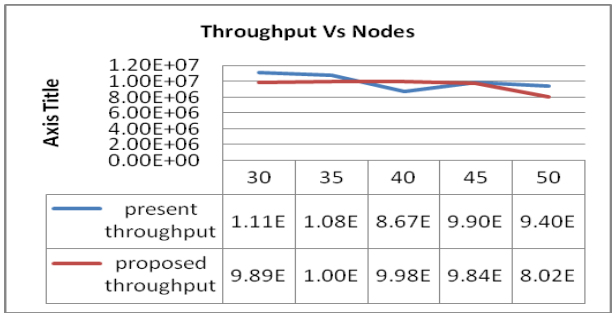

Figure 5: Throughtput Vs Number of Nodes

In fig 6, the throughtput increases with the incrase in the application rate and reaches a consistent level.Hence Proposed system rate of processing is more efficient than present sytem.

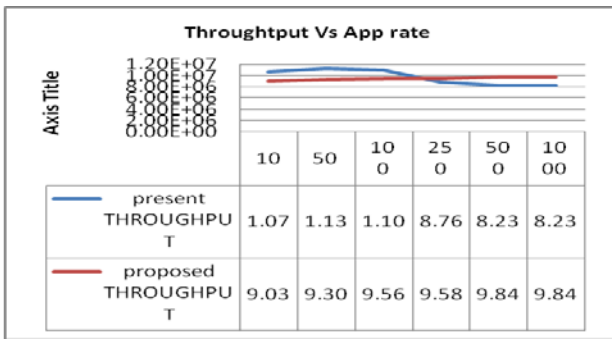

Figure 6: Throughtput Vs Application Rate

6. Conclusion and Future Work

In Manet network cluster and cluster heads are formed, it obtains the routes through nodes which are moving in the same direction of the destination. Thus path remains consistent for longer period which ensures better packet delivery and less delay. The cluster head nodes have higher degree of connectivity, and route through cluster heads goes through lesser hops, total packet transmission power loss is lesser which leads to better energy conservation and provides better performance in terms of performance parameters. The proposed system shows the simulation results of packet delivery ratio, latency, energy, throughtput by comparing with the Current system wherein it reduces latency, increases packet delivery ratio to a great deal and, the network packet transmission is secured through communication technique “Public Key Cryptographic” using Ron Rivest, Adi Shamir and Leonard Adleman(RSA) algorithm.

Future work: Higher number of hops might have to be traversed in order to reach a destination, and there exists the possibility of having isolated clusters. Note that link costs (transmitted powers), in this context, are generally different depending on the radius of each cluster. Accordingly, incorporating the minimum power routing algorithm is crucial to limit power consumption.

References

[1] Z. Zhi and Y.K. Choong, “Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy,”Proc. Third Int’l Workshop Mobile Distributed Computing (ICDCSW), 2005.
[2] I. Aad, C. Castelluccia, and J. Hubaux, “Packet Coding for Strong Anonymity in Ad Hoc Networks,” Proc. Securecomm and Workshops, 2006.
[3] Y.-C. Hu, A. Perrig, and D.B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,” Wireless Networks, vol. 11, pp. 21-38, 2005.
[4] K.El-Khatib, L. Korba, R. Song, and G. Yee, “Anonymous Secure Routing in Mobile Ad-Hoc Networks,” Proc. Int’l Conf. Parallel Processing Workshops (ICPPW), 2003.
[5] S.Ratnasamy, B. Karp, S.Shenker, D.Estrin, R. Govindan, L.Yin, and F. Yu, “Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table,” Mobile Network Applications, vol. 8, no. 4, pp. 427-442, 2003.
[6] X.Hong, M. Gerla, G. Pei, and C.C. Chiang, “A Group Mobility Model for Ad Hoc Wireless Networks,” Proc. Second ACM Int’l Workshop Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 1999.
[7] J. Li, J. Jannotti, D.S.J. De, D.S.J. De Couto, D.R. Karger, and R.Morris, “A Scalable Location Service for Geographic Ad Hoc Routing,” Proc. ACM MobiCom, 2000.
[8] J. Kong, X. Hong, and M. Gerla, “ANODR: Anonymous on Demand Routing Protocol with Untraceable Routes for Mobile Ad-Hoc Networks,” Proc. ACM MobiHoc, pp. 291-302, 2003.
[9] L. Yang, M. Jakobsson, and S. Wetzel, “Discount Anonymous On Demand Routing for Mobile Ad Hoc Networks,” Proc. Secure command Workshops, 2006.
[10] Y.-C. Hu, D.B. Johnson, and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks,” Proc. IEEE Workshop Mobile Computing Systems and Applications (WMCSA), 2002.