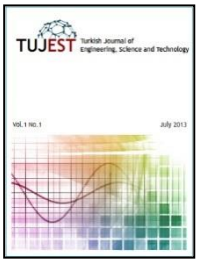
Turkish Journal of Engineering, Science and Technology 01 (2014) 31-36

TUJEST

Turkish Journal of Engineering, Science and Technology

journal homepage: www.tujest.com



Energy Efficient location privacy preserving based data transfer using LAR method in Mobile network

S. Yuva Sri[a,*], A. Kathirvel[b], S. T. Lenin[c]

[a]*Department of Information Technology, Vivekanandha College of Engineering for women, Thiruchengode, India*

Article Info

Article history:
Received December 15, 2013
Accepted February 04, 2014
Available online February 13, 2014

Keywords:
LAR,
EELPP,
NS2,
OTCL,
MAC

Abstract

To introduce an Energy Efficient Location Privacy Preserving (EELPP) Protocol for MANETs that is based on the Location Aided Routing (LAR). LAR makes significant reduction in the energy consumption of the mobile nodes batteries by limiting the area of discovering a new route to a smaller zone. Thus, control packets overhead are significantly reduced. In EELPP a reference wireless base station is used and the network's circular area centered at the base station is divided into six equal sub-areas. At route discovery instead of flooding control packets to the whole network area, they are flooded to only the sub-area of the destination mobile node. The base station stores locations of the mobile nodes in a position table. To show the efficiency of the proposed protocol we present simulations using NS-2. Simulation results show that EELAR protocol makes an improvement in control packet overhead and delivery ratio compared to AODV, LAR, and DSR protocols. To reduce the energy cost, nodes are active only during data transmission and the intersection of node creates a larger merged node, to reduce the number of fake packets and also boost privacy preservation. Simulation and analytical results demonstrate that our scheme can provide stronger privacy protection than routing-based schemes and requires much less energy than data preventing based.

1. Introduction

Mobile ad hoc networks consist of wireless mobile hosts that communicate with each other, in the absence of a fixed infrastructure.1 Routes between two hosts in a Mobile Ad hoc Network (MANET) may consist of hops through other hosts in the network. Host mobility can cause frequent unpredictable topology changes. Therefore, the task of finding and maintaining routes in MANET is nontrivial. Many protocols have been proposed for mobile ad hoc networks, with the goal of achieving efficient routing [1]. These algorithms differ in the approach used for searching a new route and/or modifying a known route.

The aim of AODV route discovery is to set up a bidirectional route from the source to the destination. Route discovery works by flood the network with route request (RREQ) packets. Each node that receives the RREQ looks in its routing table to the destination or if it has a new sufficient route to the destination. If it does, it sends a unicast route reply (RREP) message back to the source; otherwise it rebroadcasts the RREQ in [3]. The RREP is routed back on a temporary reverse route that was created by the RREQ. Each node keeps track of its local connectivity, this is performed either by using periodic exchange of messages, or by using feedback from the link layer upon unsuccessful transmission.

*Corresponding Author:
Y. Sri, E-mail: yuvasrivec@gmail.com

In addition to the work related to power-efficient algorithms, Location-Aided Routing protocols such as LAR were also proposed to make informed routing decisions based on information about node locations. LAR is different from previous work related to location-aided routing in that work, when making routing decisions. To minimizing the power consumption on end-to-end routes is the main objective. In particular, the purpose of preceding algorithms is to find out a shortest-path route that reach the destination with the smallest number of middle hops at minimizing the energy consumption in transmitting a packet.

The mobile node's with the goal of decreasing routing-related overhead in mobile and ad hoc networks. It uses location information of the mobile nodes to limit the search for a new route to a smaller area of the ad hoc network which results in a significant reduction in the number of routing messages and therefore the energy consumption of the mobile nodes batteries is decreased significantly. In order to reduce the control overhead due to broadcast storm in the network when control packets are flooded into whole network.

2. Related Work

The Mobile ad hoc networks and secured data transmission phase is of crucial importance depending upon the environments like military. A new way to improve the reliability of message transmission is presented. In the open collaborative MANET environment, any node can maliciously or selfishly disrupt and deny communication of other nodes [7]. Dynamic changing topology makes it hard to determine the adversary nodes that affect the communication in MANET.

The protocol provides a way to secure message transmission by dispersing the message among several paths with minimal redundancy. The multiple routes selected are known as APS –Active Path Set. A technique for fault discovery process to identify Byzantine failures which include nodes that drop, modify, or miss-route packets in an attempt to disrupt the routing service. An adaptive probing technique detects a malicious link through binary search and according to the nodes behaviour; these links are avoided in the active path by multiplicatively increasing their weights [8]. The proposed scheme provides secure communication even with increased number of adversaries.

Many proximity-based mobile social networks are developed to facilitate connections between any two people, or to help a user to find people with matched profile within a certain distance. A challenging task in these applications is to protect the privacy the participant's profiles and personal interests [9, 10]. They design novel mechanisms, when given a preference-profile submitted by a user that search a person with matching-profile in decentralized multi-hop mobile social networks.

Our mechanisms are privacy-preserving: no participants' profile and the submitted preference-profile are exposed. Our mechanisms establish a secure communication channel between the initiator and matching users at the time when the matching user is found [5]. Our exact analysis shows that our mechanism is secure, privacy-preserving, verifiable, and efficient both in communication and computation. Extensive evaluations using real social network data and actual system implementation on smart phones show that our mechanisms are significantly more efficient then existing solutions.

In wireless sensor networks, adversaries can make use of traffic information to locate the monitored objects, e.g., to hunt endangered animals or kill soldiers. First define a hotspot phenomenon that causes an obvious inconsistency in the network traffic pattern due to a large volume of packets originating from a small area. Second, we develop a realistic adversary model, assuming that the adversary can monitor the network traffic in multiple areas, rather than the entire network or only one area. Using this model, we introduce a novel attack called Hotspot-Locating where the adversary uses traffic analysis techniques to locate hotspots.

They have cloud scheme for efficiently protecting source node location privacy against Hotspot- Locating attack by creating a cloud with an irregular shape of fake traffic [7]. To counteract the inconsistency in the traffic pattern and camouflage the source node in the nodes forming the cloud. To reduce the energy cost, clouds are active only during data transmission and the intersection of clouds creates a larger merged cloud, to reduce the number of fake packets and also boost privacy preservation. Simulation and analytical results demonstrate that our scheme can provide stronger privacy protection than routing-based schemes and requires much less energy than global-adversary-based schemes.

Recent advances in technology have motivated new application domains for wireless networks. For example, wireless sensor networks (WSNs) are used for environmental monitoring in both civilian and military settings in [3, 2]. To promise safer roads and improved driving experience, while disruption-tolerant networks (DTNs) bring low-cost best-effort connectivity to challenged environments with little or no infrastructure. At the same time, there has been a surge of interest in body-area networks (BANs) with envisaged applications in military, law enforcement, sports and medical domains. These emerging wireless networks extend the network function beyond purely personal communication and potentially offer a world of truly ubiquitous computing. One of their distinctive features is the lack of (or non-reliance on) any wired or fixed infrastructure. Nodes communicate either directly or via peers, instead of using infrastructure elements, such as base stations or access points. Since nodes themselves are responsible for forwarding messages, they play an increasingly active role in networking mechanisms.

To send a message to a destination node that is not within the transmission range of the source node, the latter uses a routing protocol. The routing strategy that we consider in this work is prediction-based routing [6]. The protocol requires

that nodes in a community compute the maximum probability that a node in the community will encounter a destination node. We presented a protocol that computes this maximum in mobile delay tolerant networks in such a manner that the individual private values are not revealed even to the nodes inside the community.

3. Proposed Approach

The mobile ad hoc network is a new model of wireless communication and has gained increasing attention from industry. As in a general networking environment, mobile ad-hoc networks have to deal with various security threats. Due to its nature of dynamic network topology, routing in mobile ad-hoc network plays a vital role for the performance of the networks. It is understandable that most security threats target routing protocols the weakest point of the mobile ad-hoc network. There are various studies and many researches in this field in an attempt to propose more secure protocols. However, there is not a complete routing protocol that can secure the operation of an entire network in every situation.

Privacy protection in routing of MANET has interested a lot of research efforts. A number of privacy-preserving routing schemes have been brought forward. The anonymous routing protocols mainly consider anonymity and partial unlink ability in MANET, most of them exploit asymmetric feature of public key cryptosystems to achieve their goals. Complete unlink ability are not guaranteed due to incomplete content protection. This method use Energy Efficient Location Privacy Preserving Protocol (EELPP) that is an optimization to the Location Aided Routing (LAR). EELPP makes significant reduction in the energy consumption of the mobile nodes batteries through limiting the area of discovering a new route to a smaller zone. Thus, control packets overhead are significantly reduced and the mobile nodes life time is increased.

To show the efficiency of the proposed protocol we presented simulations using NS-2. In addition, simulation results show that there is a tradeoff between decreasing control overhead by increasing number of areas and increasing route loss by increasing the number of network areas due to node mobility. This suggests that optimal number of network area is dependent on the nodes mobility. We have to take a different parameters like as throughput, delivery ratio, packet delay on the network. In as much as all these protocols strived to reduce power consumption either at node level or on the network in general, all proposed solutions have a kind of trade-off that let go to have obvious energy saving. The observed performance metrics based on the simulation results posted by the various algorithms under review. The number of routes established during route discovery, the message overheads the cost of performing the data packet transmission and reception by different nodes, average energy conserved, the network throughput, the end-to-end data packet delay.

3.1. ENERGY EFFICIENT LOCATION PRIVACY ALGORITHM

(i). Energy based Packet Transmit

```
Step 1: If (Any Packet sent P)
        {
        Forward Packet P
        }
Step 2: If (received A Packet)
       {
Step 3: If (Received Packet==Data_Ack)
       {
Step 4: Route Location base transmission
          Verify the Id
Step 5: If (Verification Successful)
        Energy save mode
        {
Step 6: Discard the route noted
        Else
       {
Step 7: Drop the packet
         Energy loss
       }
Step 8: Repeat the procedure for next packet
        }
        }
```

(ii). Energy based Packet Receive

```
Step 1: If (Received a packet P)
        {
          Verify the Original data
Step 2: If (Verification Successful)
           Verify the location id model
Step 3: If (Verification Successful)
        {
          Noted route=Null;
        }
          Else
        {
Step 4: Noted Route unchanged
         }
Step 5: Create Data_Ack Packet
         Data_Ack
     }
}
```

Energy Efficient Location Privacy Preserving Algorithm Explanation

- The data are sending by wireless mobile ad-hoc network from source (S) to destination (D) on network topology.
- The Packets (P) transmit the data to destination intermediately work through from source to destination Energy efficient based transmission on network.
- Neighbor discovery node has to gather the data sending and receiving process on the network. The traffic conditions to be checked on mobility node.
- The minimum number of connected set to the destination on the network. It's more to save the energy and shortest path route discovery on their network.
- It is reducing the packet's delay and the reduce energy model on their wireless mesh network. The connected set is more efficient and scalable network on that time of the network process.

4. Performance Analysis

The goal of the simulation is to analyze the behavior of the AODV by deploying Networks. The simulation environment is creating in NS-2, a network simulator that provides support for simulating mesh wireless networks. NS-2 using C++ language and it uses the Object Oriented Tool Command Language (OTCL). It came as from Tool Command Language (TCL). They use an environment consisting of 30 wireless nodes roaming over a simulation area of 1200 meters x 1200 meters flat space operating for 10 seconds of simulation time. The radio and IEEE 802.11 MAC layer models used. Nodes in our simulation move according to Random Waypoint mobility model, which is in random direction with maximum speed from 0 m/s to 20 m/s. A free space propagation channel is unspecific for the simulation. Hence, the simulation experiments do not account for the overhead produced when a multicast member leaves a group and the comparison result.

Table 1: Simulation Parameters

PARAMETERS	VALUE
Version	Ns-allinone 2.28
Propagation Model	Two Ray Ground
Routing Protocols	AODV
Area	1200m x 1200m
Broadcast Area	50-250 m
Transfer Pattern	UDP,CBR
Mobility Model	Random Mobility
Transfer per Packet	512 bytes

5. Performance Results

The simulation scenario is calculated particularly to charge the collision of system concentration on the presentation of the network model. The collision of arrangement density is deploying 0 – 100 nodes more than a permanent open area topology of 1200m x 1200m using 5m/s node speed and identical source-destination connections. AODV have a quantity of metrics that can be used for their performance network.

Table 2: Simulation Result

No	Nodes	Method	Throughput	Avg Delay	Energy
1.	0-100	SDP	0.80	15.00	12 joule
2.	0-100	EELP	0.92	9.00	8 joule

5.1. Throughput Performance

This is the output of total number of received data packets divided by total number of sent data packets.

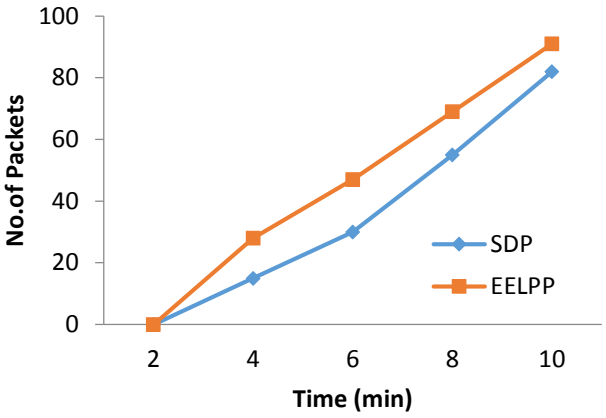


Fig1. Performance of throughput

This metric gives an estimate of how efficient a routing protocol is, since the number of routing packets sent per data packet gives an idea of how well the protocol keeps the routing information updated. The higher the Normal Routing Load metric is, the higher the overhead of routing packets and consequently the lower the efficiency of the protocol.

5.2. Energy Level on Network

The energy level on the network is must and most important one of the quick data transmission on their network. its calculated from their each node energy consumption is must of the network. if any node none to data transmit that node to save the energy on the network.

Energy consumption = no of packets * initial energy level
Remained energy = energy consumption – no of packets in node

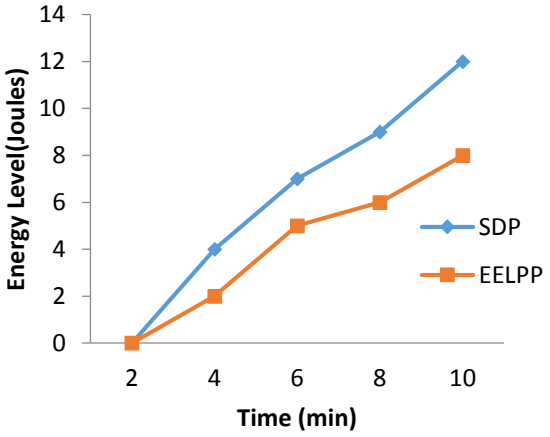


Fig3. Energy Consumption On Network

5.3. The End-to-End delay:

They have calculate a average number of delay on network, it includes all possible delay caused by buffering through route detection latency, queuing at the border queue, retransmission delay on medium access control, spread and move time.

$$D = (Tr - Ts)$$

Where Tr is receive Time and Ts is sent Time.

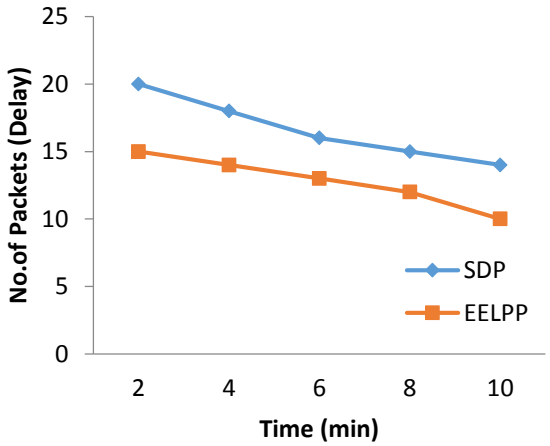


Fig3. End to End Delay on network

6. Conclusion

In our work we have using a neighbor discovery data collection to data transfer protocols for energy-efficient data gathering. Mobi-cluster uses logical coordinates to infer distances, and establishes data reporting routes by greedily selecting the shortest path to the destination reference. In addition, mobile node is capable of tracking multiple mobile sinks simultaneously through multiple logical coordinate spaces. Using Energy Efficient Location Privacy Preserving Protocol (EELPP) that is an optimization to the Location Aided Routing (LAR) for location based data transmission on their network. It has mainly focused on this method to improve the network performance and energy consumption model on the network. In our future work to implement the network protocol based energy efficient data transmission and more security based data transmission on the network. Used Security based routing protocols and reduces data loss on the network.

References

1. Mohammad A. Mikki, "Energy Efficient Location Aided Routing Protocol for Wireless MANETs", Vol. 4, No. 1 & 2, 2009.
2. P. Thamizharasi, D.Vinoth, "Unobservable Privacy-Preserving Routing in MANET", Volume-2, Issue-3, January 2013.
3. Karim El Defrawy, Gene Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANETs", VOL. 29, Dec 2011
4. Ajay Shah, Hitesh Gupta, "Energy Efficient Routing Protocols for Mobile Ad Hoc Networks", Vol. 1 Issue 5, July – 2012.
5. Mohamed M. E. A. Mahmoud, "A Cloud-Based Scheme for Protecting Source-Location Privacy against Hotspot-Locating Attack in Wireless Sensor Networks", 2011
6. K. Vinoth Kumar, G.Arunsathish, "Privacy-Preserving Routing Protocol for Mobile Ad Hoc Networks", Vol.11, No.11, March 2013.
7. Humaira Nishat, "Energy Efficient Routing Protocols for Mobile Ad Hoc Networks", Volume 26– No.2, July 2011
8. J. Haas, "Secure Data Communication in Mobile Ad Hoc Networks", VOL. 24, NO. 2, FEB 2006
9. Young-Bae KO, "Location-Aided Routing (LAR) in mobile ad hoc networks", science publication university
10. Panagiotis, Papadimitratos, "Secure Data Transmission in Mobile Ad Hoc Networks", 19 Sep 2010.