ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

An Efficient Multipath Erasure Coding based Secure Routing Protocol in Manet

K.R.Melbha[*1], J.Venkatesh[2]

[*1,2] PG Student, Department of IT, Velammal Engineering College, Chennai- 600066, Tamil Nadu, India

melbhakr@gmail.com

Abstract

Mobile ad hoc network have been developed to afford various levels to provide secrecy protection. However existing anonymous routing protocol overcome the challenges such as high energy consumption due to acknowledgement free communication and data loss due to link breakage. By using Hierarchical zone partition it provides secure communication by hiding node identities and preventing traffic analysis attacks from outside observes. Information carriage is resolved by using multipath erasure coding i.e. split the data into two path and then GPSR algorithm, find the shortest path and then send the data to destination node. It achieves better route anonymity protection and low cost compared to the previous routing protocol.

Keywords: Hierarchical zone partition, GPSR algorithm, random forwarder, destination privacy, multipath erasure coding.

Introduction

MANETs are mobile; they make use of wireless links to connect various networks. MANETs are a kind of Wireless ad hoc network [6] that usually has a energetic networking environment on top of a connection layer ad hoc network. Each device in a MANET is free to move independently in any path Each must promote traffic unrelated to its own use. Each device continuously maintains the information connected to larger Internet.

An ad hoc network is a type of provisional system to system connection. In ad hoc mode set up a wireless link [7] directly to another computer without having to connect to a wireless access point or router. An ad hoc network classically refers to any set of networks where all devices have equal status on a network and are free to connect with any other ad hoc network devices in link range. Frequently, ad hoc network refers to a mode of procedure of IEEE 802.11 wireless networks [8].

The current approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources because public key based encryption and high traffic generate significantly high cost. Many approaches cannot provide all of the anonymity protection. ALERT cannot protect the location anonymity of source and destination. ALERT only focuses on destination anonymity. Anonymity direction-finding protocols in MANETs can be mainly classified into two categories.

Hop-by-hop encryption: In hop-by-hop encryption steering, [3],[5] a packet is encrypted in the communication of two nodes direction, preventing adversaries from tampering or analyzing the packet contents to interrupt the communication or identify the two communicating nodes. The disadvantages of hop-by-hop encryption methods are that they generate high cost due to the use of hop-by-hop public-key cryptography or complex symmetric key cryptography.

Redundant traffic-based routing: It based routing such as multicast, [7],[8] local broadcasting, and flooding, to obscure potential attackers. A disadvantage of redundant traffic-based methods is the very high overhead incurred by the redundant actions or packets, leading to high cost.

An anonymous location based and efficient routing protocol in order to provide high anonymity protection with low cost. Hierarchically zone partition dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes which form a non traceable route. Specifically in each direction-finding step, a data sender or forwarder partitions the network field in order to separate itself and the destination into two zones. It then arbitrarily chooses a node in the other zone as the

ISSN: 2277-9655
Impact Factor: 1.852

next relay node and uses the GPSR algorithm to send the data to the spread node. In the last step, the data is broadcasting to k nodes in the destination zone, provided that k-anonymity to the target. In addition, this strategy hides the data initiator among a number of initiators to strengthen the anonymity protection of the source. Anonymous location is also resilient to intersection attacks and timing attack. This project theoretically analyzed protection in terms of anonymity and efficiency. This scheme also conducted experiments to evaluate the performance of hierarchically zone partition in comparison with other anonymity and geographic routing protocol. It increases the user privacy and delivery ratio is high.

Related Work

In all existing work anonymity can be applied to different network models with various node movement patterns such as random way point model [9] and group mobility model [5]. Consider a MANET deployed in a large field where geographic routing is used for node communication in order to reduce the message latency. The location of a message's dispatcher may be revealed by merely exposing the broadcast direction. Therefore, an nameless communication protocol that can afford untraceable is required to strictly ensure the secrecy of the sender.

Moreover,a malicious[2] observer may try to block the data packets by compromising the amount of nodes, interrupt the packets on amount of nodes, or even trace back to the dispatcher by detecting the data transmission direction. Therefore, the direction should also be undetectable.

A malicious observer may also try to detect destination nodes through traffic analysis by launching an intersection attack. Therefore, the destination node [5] also needs the protection of secrecy. In this work, the attackers can be battery powered nodes that inactively receive network packets and detect activities in their area. They can also be powerful nodes that pretend to be legitimate nodes and inject [7] packets to the network according to the logical results from their attic dropped packets. The assumptions under apply to equally inside and outside attackers.

Capabilities: By eavesdropping, the adversary nodes can analyze any direction-finding protocol and obtain in-formation about the communication packets in their area and positions of other nodes in the network. They can also monitor data communication on the fly when a node is communicating with other nodes and record the historical communication of nodes. They can interrupt on some specific vulnerable nodes to control their behavior, e.g., through denial-of-service (DoS) attack, which may cut the routing in existing nameless geographic direction-finding methods.

In capabilities: The attackers do not issue strong dynamic attacks such as black hole. They can only achieve intrusion to a proportion of all nodes. Their computing resources are not unrestricted; therefore, both symmetric and public/private input cannot be roughly decoded within a logical time period. Therefore, encrypted data are secure to a certain degree when the key is not known to the attackers.

Location Based Privacy

Based on the location MANET gives privacy to user and also it protect from anonymous. In a node communication, a source node sends a request to target node and the destination responds among data. A communication session is the time period that S and D interact with each other continuously until stop. Here each node uses a dynamic pseudonym as its node identifier rather than using its real MAC address which can be used to trace nodes existence in the network. To avoid pseudonym collision it use a collision resistant hash function and also public key is used to enable two nodes securely for secure communication.

MANET Model

A mobile ad hoc network (MANET) is a self-configuring infra structure less network of movable devices associated by wireless. Each device in a MANET is free to move independently in any path, and will therefore change its relations to other devices frequently. MANETs are a type of Wireless ad hoc network . As for the mode of procedure, ad hoc networks are basically peer-to-peer alternative-hop mobile wireless networks where information packets are transmitted in a store-and-forward manner from a source to a destination, via middle nodes.

Location Service

A locality check enables a supply node, which is aware of the identity of the target node, to securely obtain the locality and public key of the target node. The public key is used to allow two nodes to securely create a symmetric key Ks for secure communication. Specifically, trusted normal nodes or dedicated service provider nodes are used to provide position check. Each node has a locality server. When a node A requests to know the location and public key of another node B, it will sign the demand containing B's identity using its individual identity. Then, the locality server of A will go back an encrypted position of B and its public key, which can be decode a message by A using the distributed shared key between A and its location server.

ISSN: 2277-9655
Impact Factor: 1.852

Hierarchically Zone Partition

The whole network area is generally a rectangle in which nodes are randomly spread. The information of the bottom-right and upper left boundary of the network area is configured into each node when it joins in the method. This information allows a node to find the positions of nodes in the whole area for zone partitions in network.

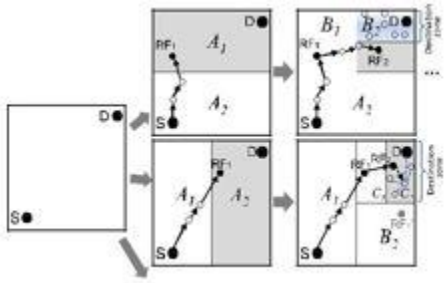

Fig.1: Hierarchically zone partition

Secret routing features a energetic and random direction-finding path, which consists of a number of energetically deter-mined intermediate relay nodes. Nodes are horizontally separation it into two zones A_1 and A_2. Then nodes vertically divide zone A_1 to B_1 and B_2. After that, we horizontally divide zone B_2 into two zones. Such zone partitioning successively splits the smallest zone in an alternating horizontal and vertical manner. This division process is called hierarchical zone partition. GPSR algorithm uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in every step as an transitional relay node (i.e., data forwarder), thus dynamically generating an unpredictable routing path for a message.

GPSR Algorithm:

As GPSR, assume that the destination node will not move extreme away from its position during the data communication, so it can effectively receive the data. A larger number of hierarchies create more direction-finding hops, which increases secrecy degree but also increases the delay. To ensure the delivery of packets, the target sends a authorization to the source upon getting the packets. If the source has not received the authorization during a predefined occasion period, it will resend the packets.

Anonymity Protection:

Each device produce provisional key and it identify the source and destination. Then only sending data is protected. So here using cryptographic techniques for source, destination and router and it will encrypt the data by use of public key. One of these two keys is used to encode the message on the sender side, another is used to decode the message on the receiver side. One of these two keys are usually kept secret; restricting access to it (private key) and another is public and can be known to everyone. RSA can be used in our proposed system, Sender uses widely known public key to encrypt the message. Only receiving person who also knows the private key can decrypt it. By this way data will secure.

.Multipath Erasure Coding:

Erasure coding is a coding technique that converts a message into a set of coded packets such that any satisfactorily large division of the coded packets can be used to recreate the original message. In this paper, assume that the original message has been divide into k equal-sized packets. From the angle of linear algebra, every packet divide from the original message can be regarded as a variable, and an erasure-coded packet is a linear combination of the k original packets. This can be expressed as a linear equation where the left hand side of the equation is the linear grouping of the k original packets, and the right hand side is the erasure-coded packet. As long as k linearly independent coded packets are given, the original message can be reconstructed by solving the k linear independent equations associated with the k coded packets.

Experiment Evaluation

For experimental result evaluated the destination based privacy in fig.2.This figure depicts the number of nodes moving speed when the node density equals and also it shows the number of remaining nodes with different numbers of partitions and node moving speed.

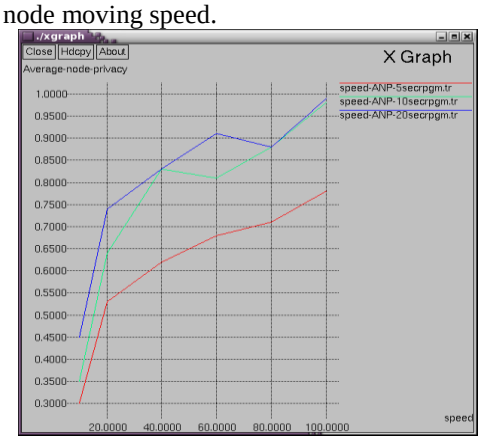

Fig.2: Performance result about speed

Here we fixed the number of nodes in destination zones and set the data transmission. Therefore destination anonymity is represented as a function of both node speed and density. Here the node speed increases, the necessary node density also increases. This is logical because earlier movement blanks out nodes originally in the destination zone more quickly.

ISSN: 2277-9655
Impact Factor: 1.852

Conclusion

In this project GPSR algorithm is eminent by its low cost and anonymity protection for sources, destinations and routes. It uses energetic hierarchical zone partitions and random relay node selections to create it difficult for an intruder to identify the two endpoints and nodes en route. A packet in unknown location includes the source and destination zones rather than their positions to provide secrecy protection to the source and the destination. It can also achieve similar direction-finding efficiency to the base line GPSR algorithm. Using multi path erasure coding technique, that converts a message into a set of coded packets such that any suitably large subset of the coded packets can be used to reconstruct the original message. This technique will provide energy efficient and high packet delivery ratio.

References

[1] *Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks," Proc. Int'l Symp. Applications on Internet (SAINT), 2006.*

[2] *Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Proc. Third Int'l Work-shop Mobile Distributed Computing (ICDCSW), 2005.*

[3] *V. Pathak, D. Yao, and L. Iftode, "Securing Location Aware Services over VANET Using Geographical Secure Path Routing,"Proc. IEEE Int'l Conf. Vehicular Electronics and safety (ICVES), 2008.*

[4] *K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2007.*

[5] *K.E. Defrawy and G. Tsudik, "PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2008.*

[6] *A. Perrig, R. Canetti, D. Song, and J.D. Tygar, "Efficient and Secure Source Authentication for Multicast," Proc. Network and Distributed System Security Symp. (NDSS), 2001.*

[7] *M.F. Mokbel, C.-Y. Chow, and W.G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy," Proc. 32nd Int'l Conf. Very Large Databases (VLDB), 2006.*

[8] *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.*

[9] *Y. Xue, B. Li, and K. Nahrstedt, "A Scalable Location Management Scheme in Mobile Ad-Hoc Networks," technical report, 2001.*

[10] *J. Li, J. Jannotti, D.S.J. De, C. David, R. Karger, and R. Morris, "A Scalable Location Service for Geographic Ad Hoc Routing," Proc. ACM MobiCom, 2000.*

[11] *L. Sweeney, "k-Anonymity: A Model for Protecting Privacy," Int'l J. Uncertainity Fuzziness Knowledge-Based Systems, vol. 10, no. 5, pp. 557-570, 2002.*

[12] *A.R..Beresford and F.Stajano,"Mix zones:User Privacy in Location-Aware Services,"Proc.IEEE Second Ann.Conf.Pervasive Computing and comm..workshops(PERCOMW),2004.*

[13] *X.Wu,"DISPOSER:Distributed Secure Position Service in Mobile Ad Hoc Networks:Research Articles,"Wireless Comm.and Mobile Computing,vol.6,pp.357-373,2006.*

[14] *Y.Zhang, W.Liu ,and W.Luo,"Anonymous Communications in Mobile Ad Hoc Networks,"Proc.IEEE INFOCOM,2005.*

[15] *L.Sweeney,"k-anonymity:A model for protecting Privacy,"Int'l J.Uncertainity Fuzziness Knowledge-Based Systems,vol.10,no.5,pp.557-570,2002.*