SECURITY BASED ANONYMOUS EFFICIENT ROUTING PROTOCOL IN MANETs

[1]C.Muthukumar, [2]K.Ramthilak,

[1]PG Scholar, Department of ECE, Sriguru Institute of Technology, Coimbatore, India.

[2]Assistant Professor, Department of ECE, Sriguru Institute of Technology, Coimbatore, India

Abstract: Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols that hide node identifies and/or routes from outside observers in order to provide anonymity protection. However, existing anonymous routing protocols relying on either hop-by-hop encryption or redundant traffic either generate high cost or cannot provide full anonymity protection to data sources, destinations, and routes. The high cost exacerbates the inherent resources constraints problem in MANETs especially in multimedia wireless applications. To offer high anonymity protection at a low cost, we propose an Anonymous Location-based Efficient Routing Protocol (ALERT). ALERT dynamically partitions the network field into zones randomly chooses nodes in zones as intermediate relay nodes, which from a non traceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. Thus, ALERT offers anonymity protection to sources, destination, and routes. It also has strategies to effectively counter intersection and timing attacks. We theoretically analyze ALERT in terms of anonymity and efficiency .Experimental results exhibit consistency with the theoretical analysis, and show that ALERT achieves better route anonymity protection and lower cost compared to other anonymous routing protocols. Also, ALERT achieves comparable routing efficiency to the GPSR geographical routing protocol. Mainly to solve the Clone detection and outside attacks using Prevention detection technique.

Keywords: Anonymity, Anonymity protection, hop by hop encryption, Alert protocol, GPSR.

Reference to this paper should be made as follows: Author(s) (2006) 'Security Based Anonymous Efficient Routing Protocol In Manets', *International Journal of Inventions in Computer Science and Engineering*, Volume 1 Issue 3 2014

1 Introduction

A community of ad-hoc network researchers has proposed, implemented, and measured a variety of routing algorithms for such mobile, wireless networks. While these ad-hoc routing algorithms are designed to generate less routing protocol traffic than the above-mentioned shortest-path routing protocols in the face of a changing topology, they nevertheless compute shortest-path routes using either topological information concerning the entire network, or topological information concerning the entire set of currently used paths between sources and destinations. Thus, their ability to find routes depends similarly on describing the current wide-area topology of the network to routers. We propose a different strategy for routing on wireless networks than these traditional routing algorithms and ad-hoc routing algorithms use. The central approach in this thesis is to make routing decisions Klein rock, Hou and Li, and Finn. By using geographic forwarding, we exploit the facts that: Intuitively, leveraging this inherent structure in wireless networks can localize the portion of the network topology that must be described to routers in a routing protocol.

Localizing the topological information that must be communicated among routers in a routing protocol improves the scaling of routing in three ways: it reduces the absolute volume of routing protocol message traffic, reduces the size of the state that must be stored at routers, and reduces the risk that state stored at a router concerning a far-away portion of the topology will become stale. Greedy Perimeter Stateless Routing (GPSR), a routing protocol for wireless networks, which makes geographic forwarding decisions, and finds routes using knowledge at each node of only that node's immediate single-hop neighbors in the topology.

2. Related Work

A.Factor: Module Description Security based Anonymous efficient Routing protocol to find out the level of module description, which is as follows.

Node Creation: Node Creation is the first module of the project. The sensor nodes are to be deployed. Route

Discovery: ALERT provides route anonymity of source and destination. Rather than relying on hop-by-hop encryption and redundant traffic, ALERT mainly uses randomized routing of one message copy to provide anonymity protection.

Data Transmission: Transmit the data from source node to destination node through the intermediate nodes which are selected randomterly in the network zones. Attacker

Prevention: ALERT has a strategy to effectively counter intersection attacks, which have proved to be a tough open issue. ALERT can also avoid timing attacks because of its non fixed routing paths for a source-destination pair. Using "Malicious node detection" scheme to prevent the network

from Active attackers and also solved the Clone detection, outside attackers using prevention detection technique.

B. Factor: Testing Security based Anonymous efficient Routing protocol to find the testing process of executing program with intent of finding an error.

White Box Testing: All independent paths have been exercised at least once. Conditional Testing: All the resulting paths were tested.

Dataflow Testing: Selects the path of the program according to the location of definition and use of variables. Loop Testing: All the loops are tested to all the limits possible.

C. Factor: Create Network Topology Security based Anonymous efficient Routing protocol to create the network topology in Physical layer.

Physical layer: Create network topology in Physical layer. The Physical Layer is the first and lowest layer in the seven-layer OSI model of computer networking. The implementation of this layer is often termed PHY.The Physical Layer which consists of the basic hardware and bit transmission over transmission medium in network. It is a fundamental layer underlying the logical data structures of the higher level functions in a network. Due to the plethora of available hardware technologies with widely varying characteristics, this is perhaps the most complex layer in the OSI architecture.

D. Factor: Create transport connection Security based Anonymous efficient Routing protocol to create transport connection using the TCP as follows.

Transport Connection: Transport connection which performs in Transport layer. Transport layers are contained in both the TCP/IP which is the foundation of the INTERNET and the OSI model of general networking. The definitions of the Transport Layer are slightly different in these two models. This article primarily refers to the TCP/IP model, in which TCP is largely for a convenient application programming interface to internet hosts, as opposed to the OS model of definition interface.

3. Proposed Methodology

Alertfeatures a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes. Given an area, we horizontally partition it into two zones A1 and A2. We then vertically partition zone A1 to B1 and B2. After that, we horizontally partition zone B2 into two zones. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner. We call this partition process hierarchical zone partition. ALERT uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., data forwarder), thus dynamically generating an unpredictable routing path for a message.

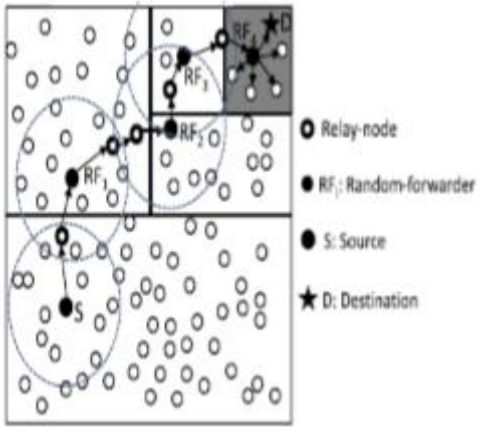

Fig 1.Proposed Alert Protocol

The packet format of ALERT, which omits the MAC header. Because of the randomized routing nature in ALERT, we have universal for RREQ/RREP/NAK. Anode uses NAK to acknowledge the loss of packets. The data field of RREQ/RREP is left blank in NAK packets. Flooding based anonymity routing usually uses ACKs, while NAKs are often adopted in geographic routing-based approaches to reduce traffic cost. For the same purpose, we choose to use NAKs. In the packet, PS is the pseudonym of a source. PD is the pseudonym of the destination; LZS and LZD are the positions of the Hth partitioned source zone and destination zone, respectively; LTD is the currently selected TD's coordinate; h is the number of divisions so far, H is the maximum allowed number of divisions; and KS s denotes the symmetric key of a source. Particularly, TTL, KRN pub is used for the protection of source anonymity and will be introduced, and Bitmap, KD pub is used for solving intersection attack. When node A wants to know the location and public key of another node B. There is no need to exchange shared keys between nodes.

A wide variety of ad-hoc routing algorithms have been proposed in the literature. By way of introduction, we focus on Dynamic Source Routing (DSR).

We compare GPSR with DSR later in the thesis, because DSR has been shown to perform better than many other published routing algorithms. In DSR, packets are routed using source routes; each packet contains the full sequence of hops it is to take from the source node to the destination node. Forwarding such a packet amounts to finding the next hop in the list of hops, and sending the packet to the appropriate neighbor.

Packet departure and arrival times, an intruder can identify the packets transmitted between S and D, from which it can finally detect S and D. Two nodes A and B communicate with each other at an interval of 5 seconds. After a long observation time, the intruder finds that A's packet sending time and B's packet receiving time have a fixed five second difference such as (19:00:55, 19:01:00) and (20:01:33, 20:01:38). Then, the intruder would suspect that A and B are communicating with each other. Avoiding the exhibition of interaction between communication nodes is a way to

counter timing attacks. In ALERT, the "notify and go" mechanism and the broadcasting in ZD both put the interaction between S-D into two sets of nodes to obfuscate intruders. More importantly, the routing path between a given S-D and the communication delay (i.e., time stamp) change constantly, which again keeps an intruder from identifying the S and D. In an intersection attack, an attacker with information about active users at a given time can determine the sources and destinations that communicate with each other through repeated observations.

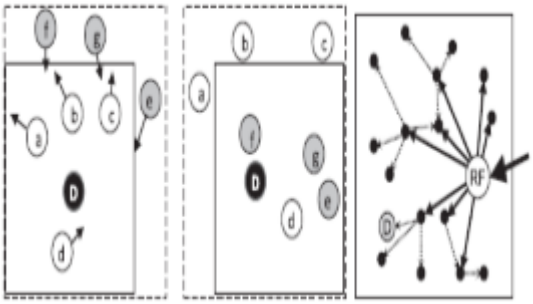

Fig 2.Resilience to Timing Attacks

Counter Intersection Attacks: In an intersection attack, an attacker with information about active users at a given time can determine the sources and destinations that communicate with each other through repeated observations. Intersection attacks are a well-known problem and have not been well resolved. Though ALERT offers k-anonymity to D, an intersection attacker can still identify D from repeated observations of node movement and communication if D always stays in ZD during a transmission session. This is because as long as D is conducting communication, the attacker can monitor the change of the members in the destination zone containing D. As time elapses and nodes move, all other members may move out of the destination because it always appears in the destination zone.

Fig 2 is the status of a ZD after the packet is broadcasted to the zone. The arrows show the moving directions of nodes. We can see that nodes a, b, c, d, and D are in ZD. It is the subsequent of the status in the next time a packet is transmitted between the same S-D pair. This time, nodes d, e, f, g and D are in ZD. Since the intersection of the in-zone nodes in both figures includes d and D, D could be identified by the attacker. Therefore, the longer an attacker watches the process, the easier it is to identify the destination node.

Fig. 2 shows the two-step process with the first step in solid arrows and the second step in dashed arrows. We can see that the first step reaches a number of nodes in the destination zone, but the destination is reached in the second step. Because the deliveries of packet1 and packet2. Therefore, the attacker would think that D is not the recipient of every packet in ZD in the transmission session, thus foiling the intersection attack.

Clone detection attacker means one node is also same as to another node and at the same time any other node is inside to another node. So, the attacker is easy to attack the node. Outside attacker also to attack this level, these two attacks are solving using the Prevention detection technique. This is measured to check the distance, IP address for outside node to entry on the circle, if it is correct the process are continue.

4. Performance Evaluation

The simulation model is implemented using the TCL language. TCL did not originally have object oriented (OO) syntax (8.6 provides an OO system in TCL core), so OO functionality was provided by extension packages, such as incr. TCL and XOTCL. Even purely scripted OO packages exist, such as Snit and STOOOP (simple TCL-only object-oriented programming).

Safe-TCL is a subset of TCL that has restricted features. File system access is limited and arbitrary system commands are prevented from execution. It uses a dual interpreter model with the "un trusted interpreter" running code in an un trusted script.

To include active messages in email. Safe-TCL can be included in e-mail when the application/safe-TCLamultipart/enabled-mail are supported. The functionality of Safe-TCL has since been incorporated as part of the standard TCL/TK releases.

The operating system are used in to the UBUNTU 10.04, the network simulator tool NS 2.34 used. The tool command language to simulate the time is 50. The total network area should be covered as to the 500 x 500 area. The numbers of nodes are 50. The bandwidth is used in that the level as 11MB, Interface Queue Length is 100, and using the alert protocol to find the simulation results.

OPERATING SYSTEM	**UBUNTU10.04**
Tool	**MS 2.34**
Language	**TCL**
Simulation Time	**50**
Network Area	**500X500**
Number of Nodes	**50**
Frequency	**2.472c9**
Receiver Threshold Value	**2.62861e-09**
Bandwidth	**11MB**
Interface Queue Length	**100**
Routing Protocol	**ALERT**

Table 1 Execution Time and Performance of Operations

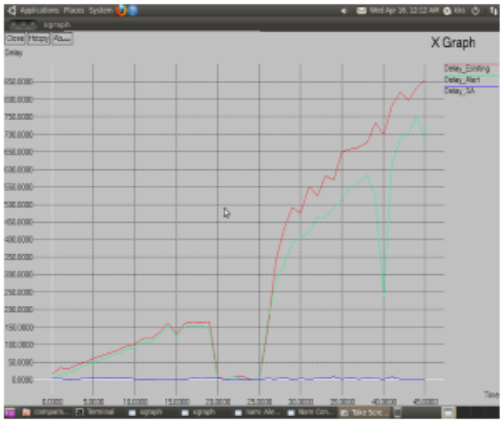

Fig 3.Output of Delay

Fig 3 shows the time and delay period of Alert protocol to existing system and Security based anonymous efficient routing protocol. In this level of alert using ad hoc routing algorithms and using DSR the delay time is decreased, at the same time by using Prevention detection technique to more level of delay is reduced of security based Anonymous efficient routing protocol. The time is measured at the distance is 0, 5, 10, 15…45. The Delay level are represented by the 0, 50,…850.

Fig 4 shows the Packet delivery ratio, (PDR)the source node to send the data to the destination node, the source node to choose the node as intermediate relay node and the node are send the data on to the hierarchical zone partitions. ALERT uses the hierarchical zone partition and dynamically generating an unpredictable routing path for a message. So, the PDR is most important to send the data on source to the destination. The Security based Anonymous routing protocol to better level of send data to the destination.

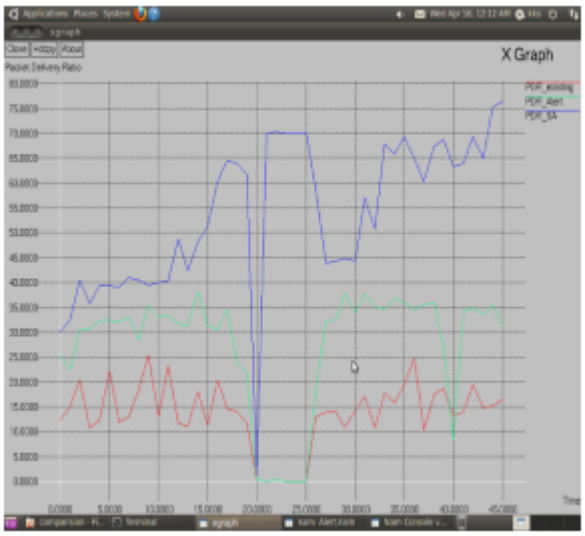

Fig 4.Output of PDR(Packet Delivery Ratio)

5. Conclusion And Future Work

Previous anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, generate high cost. Also, some protocols are unable to provide complete source, destination, and route anonymity protection. ALERT is distinguished by its low cost and anonymity protection for sources, destinations, and routes. It uses dynamic hierarchical zone partitions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route.

A packet in ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination.

ALERT further strengthens the anonymity protection of source and destination by hiding the data initiator/receiver among a number of data initiators/receivers. It has the "notify and go" mechanism for source anonymity, and uses local broadcasting for destination anonymity. In addition, ALERT has an efficient solution to counter intersection attacks. ALERT's ability to fight against timing attacks is also analyzed. Experiment results show that ALERT can offer high anonymity protection at a low cost when compared to other anonymity algorithms. It can also achieve comparable routing efficiency to the base- line GPSR algorithm. Like other anonymity routing algorithms, ALERT is not completely bulletproof to all attacks. Future work lies in reinforcing ALERT in an attempt to thwart stronger, active attackers and demonstrating comprehensive theoretical and simulation results and to solve the clone detection, outside attackers using the prevention technique based on Security based Alert system in MANET's. In clone detection and outside attackers are solved using prevention detection technique.

This project, the existing level is only solved as to the timing and counter intersection attacks. The proposed levels are solved to the Clone detection attacks and outside attacks are solved as to the Security based Anonymous efficient routing protocol. The main future work is to send the data on randomly and unpredictable routing path and also many other attacks are available, using to increase the high efficient.

References

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

[2] Beresford. A.R and Stajano. F, "Mix Zones: User Privacy in Location-Aware Services," Proc. IEEE Second Ann. Conf. Pervasive Computing and Comm. Workshops (PERCOMW), 2004.

[3] Camp. T, Boleng. J, and Davies.V, "A Survey of Mobility Models for Ad Hoc Network," Wireless Communications and Mobile Computing, vol. 2, pp. 483-502, 2002.

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

[5] El- Khatib. K, Korba. L, Song. R and Yee. G, "Anonymous Secure Routing in Mobile Ad-Hoc Networks,"

Proc. Int'l Conf. Parallel Processing Workshops (ICPPW), 2003.
[6] Frey.H and Stojmenovic.I, "On Delivery Guarantees of Face and Combined Greedy-Face Routing in Ad Hoc and Sensor Networks," Proc. ACM MobiCom, 2006.
[7] Hu.Y-C, Perrig. A and Johnson. D.B, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, pp. 21-38, 2005.
[8] Lee. K.C, Haerri. J, Uichin. L and Gerla. M, "Enhanced Perimeter Routing for Geographic Forwarding Protocols in Urban Vehicular Scenarios," Proc. IEEE Globe Com Workshops, 2007.
[9] Zhao. L and Shen. H, "ALERT: An AnonymousLocation-Based Efficient Routing Protocol in MANETs," Proc. Int'l Conf. Parallel Processing (ICPP), 2011.
[10] Zhu. B, Wan. Z, Kankanhalli, Bao. M.S.F and Deng. R.H, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc.IEEE 29th Ann. Int'l Conf. Local Computer Networks (LCN), 2004

Author Profile

Mr.C.Muthukumar Pursuing Master of Engineering (Final Year) under Anna University in Communication Systems in Sriguru Institute of Technology, Coimbatore,T.N, India. Received Bachelor of Engineering (2012) under Anna University in Electronics and Communication Engineering in KTVR-Knowledge Park for Engineering and Technology, Coimbatore, T.N, India. His interested area includes Network security management and Network routing algorithms. .