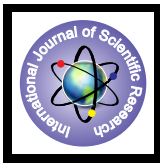
Volume : 3 | Issue : 5 | May 2014 • ISSN No 2277 - 8179

Research Paper

WRP: A Wellwisher Routing Protocol in MANETs



Engineering

KEYWORDS :

Shubi K G | Final Year M.Tech CSE, Vedavyasa Institute of Technology,Calicut

ABSTRACT

A mobile ad-hoc network is a self configuring infrastructure less network of mobile devices connected in a wireless manner. Anonymity is a state of being not identifiable within a set of subjects. MANETs make use of anonymous routing protocols in order to provide anonymity protection. Either hop-by-hop encryption or redundant traffic methods are used in existing anonymous routing protocol .But they either generate high cost or cannot provide full anonymity protection. ALERT Anonymous Location Based Efficient Routing Protocol is a new protocol for providing high anonymity protection at low cost. Network is portioned into zones in a dynamic manner. This protocol provides

1) source anonymity, 2) destination anonymity and 3) route anonymity. Simulation result of ALERT proves that this protocol performs better compared to existing protocols like GPSR. But still this protocol does not provide security to black hole attack

Introduction

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. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary 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 can be used for facilitating the collection of sensor data mining for a variety of applications such as air pollution monitoring and different types of architectures can be used for such applications. The key characteristic of such applications is that nearby sensor nodes monitoring an environmental feature typically registers similar values. This kind of data redundancy due to the spatial correlation between sensor observations inspires the techniques for in-network data aggregation and mining. By measuring the spatial correlation between data sampled by different sensors, a wide class of specialized algorithms can be developed to develop more efficient spatial data mining algorithms as well as more efficient routing strategies.

Opposed to infrastructed wireless networks where each user directly communicates with an access point or base station, a MANET, does not rely on fixed infrastructure for its operation. The network is autonomous transitory association of mobile nodes that communicate with each other over wireless links. Nodes that lie within each other's send range can communicate directly and are responsible for dynamically discovering each other. In order to enable communication between nodes that are not directly within each other's range, intermediate nodes act as routers that relay packets generated by other nodes to their destination. These nodes are often energy-constrained-that is, they are battery powered devices with great diversity in their capabilities. Furthermore, devices are free to join or leave the network and they may move randomly, possibly resulting in rapid and unpredictable topology changes. In the energy constrained dynamic, distributed multi-hop environment, nodes need to organise themselves dynamically in order to provide the necessary network functionality in the absence of fixed infrastructure or central administration. Despite the design constraints, mobile ad hoc networks offer numerous advantages. First of all, this type of network is highly suited for use in situations where a fixed infrastruure is not available, not trusted, too expensive or unreliable. Also, ad hoc networks do not need to operate in standalone fashion, but can be attached to the internet, thereby integrating many different devices and making their services available to other users. Furthermore, capacity range and energy arguments promote their use in tandem with existing cellular infrastructures as they can extend coverage and interconnectivity. As a consequence mobile ad hoc networks are expected to become an important part of the future 4G architecture which aims to provide pervasive computer environments that support users in accomplishing their tasks, accessing information and communicating anytime, anywhere and from any device.

2.11 SUMMARY

In this chapter various comparison studies are discussed which are done by different authors and different types of routing methods were discussed.

PROPOSED WORK

Networks and Attack Models and Assumptions ALERT can be applied to different network models with various node movement patterns such as random way point model and group mobility model. Consider a MANET deployed in a large field where geographic routing is used for node communication in order to reduce the communication latency. The location of a message's sender may be revealed by merely exposing the transmission direction. Therefore, an anonymous communication protocol that can provide untraceability is needed to strictly ensure the anonymity of the sender when the sender communicates with the other side of the field. Moreover, a malicious observer may try to block the data packets by compromising a number of nodes, intercept the packets on a number of nodes, or even trace back to the sender by detecting the data transmission direction. Therefore, the route 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 also needs the protection of anonymity. In this work, the attackers can be battery powered nodes that passively receive network packets and detect activities in their vicinity. They can also be powerful nodes that pretend to be legitimate nodes and inject packets to the network according to the analytical results from their eavesdropped packets.

3.2 DYNAMIC PSEUDONYM AND LOCATION SERVICE

In one interaction of node communication, a source node S sends a request to a destination node D and the destination responds with data. A transmission session is the time period that S and D interact with each other continuously until they stop. In ALERT, 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, we use a collision resistant hash function, such as SHA-1 , to hash a node's MAC address and current time stamp. To prevent an attacker from recomputing the pseudonym, the time stamp should be precise enough (e.g., nanoseconds). Considering the network delay, the attacker needs to compute, e.g., 105, times for one packet per node. There may also be many nodes for an attacker to listen, so the computing overhead is not acceptable, and the success rate is low. To further make it more difficult for an attacker to compute the times tamp, they can increase the computation complexity by using randomization for the time stamps. Specifically, they keep the precision of time stamp to a certain extent, say 1 second, and randomize the digits within 1/10th. Thus, the pseudonyms cannot be easily reproduced. A node's pseudonym expires after a specific time period in order to

Volume : 3 | Issue : 5 | May 2014 • ISSN No 2277 - 8179

prevent adversaries from associating the pseudonyms with nodes. If pseudonyms are changed too frequently, the routing may get perturbed; and if pseudonyms are changed too infrequently, the adversaries may associate pseudonyms with nodes across pseudonym changes. Therefore, the pseudonym changing frequency should be appropriately determined. Each node periodically piggybacks its updated position and pseudonym to "hello" messages, and sends the messages to its neighbours. Also, every node maintains a routing table that keeps its neighbours pseudonyms associated with their locations. As previous works, they assumed that the public key and location of the destination of a data transmission can be known by others, but its real identity requires protection. They caould utilize a secure location service , to provide the information of each node's location and public key. Such a location service enables a source node, which is aware of the identity of the destination node, to securely obtain the location and public key of the destination node. The public key is used to enable two nodes to securely establish a symmetric key K for secure communication. The destination location enables a node to determine the next hop in geographic routing. Specifically, trusted normal nodes or dedicated service provider nodes are used to provide location service. Each node has a location server. When a node A wants to know the location and public key of another node B, it will sign the request containing B's identity using its own identity. Then, the location server of A will return an encrypted position of B and its public key, which can be decrypted by A using the predistributed shared key between A and its location server. When node A moves, it will also periodically update its position to its location server. For high reliability, the location serves can replicate data between each other. Thus, the location servers are allowed to fail, because each node can be in contact with all location servers in range.

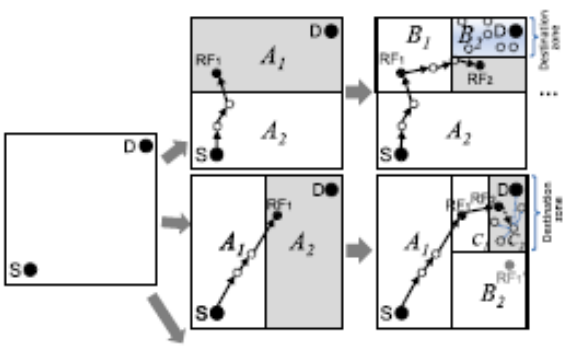


Fig 3.1 Examples of different zone partitions

The existence of the location servers are opposed to the ad hoc property of MANETs, and it is not necessary to use For ease of illustration, They assumed the entire network area is generally a rectangle in which nodes are randomly disseminated. The information of the bottom-right and upper left boundary of the network area is configured into each node when it joins in the system. This information enables a node to locate the positions of nodes in the entire area for zone partitions in ALERT.ALERT features a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes. In the figure 3.1, given an area, is partioned horizontally it into two zones A1 and A2. After that they then vertically partitioned the zone A1 to B1 and B2. Again they horizontally partitioned zone B2 into two zones. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner.They called this partition process as 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.

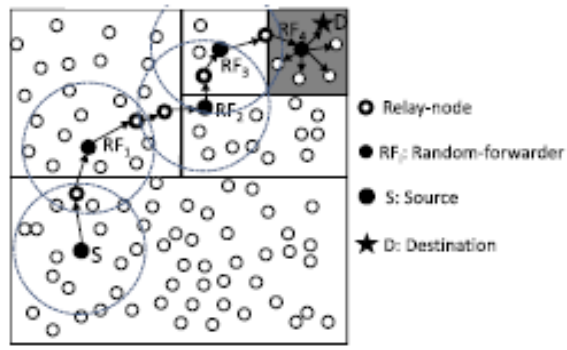


Fig 3.2 Routing among zones in ALERT

Fig. 3.2 shows an example of routing in ALERT. The zone ha' Z_D k nodes where D resides the destination zone, denoted as . k is used to control the degree of anonymity protection for the destination. The shaded zone in Fig. 2 is the destination zone. Specifically, in the ALERT routing, each data source or forwarder executes the hierarchical zone partition.

It first checks whether itself and destination are in the same zone. If so, it divides the zone alternatively in the horizontal and ical directions. The node repeats this process until itself and Z_D are not in the same zone. It then randomly chooses a position in the other zone called temporary destination (TD), and uses the GPSR routing algorithm to send the data to the node closest to TD. This node is defined as a random forwarder (RF). Fig. 3 shows an example where node N3 is the closest to TD, so it is selected as a RF. ALERT aims at achieving k anonymity for destination node D, where k is a predefined integ hus, in the last step, the data are broadcasted to k nodes in Z_D, providing k-anonymity to the destination.

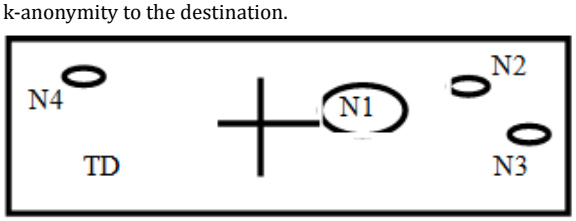


Fig 3.3 Choosing an RF according to the given TD

Given an S-D pair, the partition pattern in ALERT varies depending on the randomly selected TDs and the order of horizontal and vertical division, which provides a better anonymity protection. Fig. 1 shows two possible routing paths for a packet pkt issued by sender S targeting destination D in ALERT. There are also many other possible paths. In the upper routing flow, data source S first horizontally divides the area into two equal-size zones, A1 and A2, in order to separate S and Z_D. S then randomly selects the first temporary destination TD1 in zone A1 where Z_D resides. Then, S relies on GPSR to send pkt to TD1. The pkt is forwarded by several relays until reaching a node that cannot find a neighbor closer to TD1. This node is considered to be the first random-forwarder RF1. After RF1 receives pkt, it vertically divides the region A1 into regions B1 and B2 so that Z_D and itself are separated in two different zones. Then, RF1 randomly selects the next temporary destination TD2 and uses GPSR to send pkt to TD2. This process is repeated until a packet receiver finds itself residing in Z_D, i.e., a partitioned zone is Z_D having k nodes. Then, the node broadcasts the pkt to the k nodes. The lower part of Fig. 1 shows another routing path based on a different partition pattern. After S vertically partitions the whole area to separate itself from Z_D, it randomly chooses TD1 and sends pkt to RF1. RF1 partitions zone A2 into B1 and B2 horizontally and then partitions B1 into C1 and C2 vertically, so that itself and Z_D are separated. Note that RF1 could vertically partition A2 to separate itself from Z_D in two zones but may choose a TD further away from the destination than the TD that resulted from the horizontal

partition. Therefore, ALERT sets the partition in the alternative horizontal and vertical manner in order to ensure that a pkt approaches D in each step. As GPSR, they assumed that the destination node will not move far away from its position during the data transmission, so it can successfully receive the data. In this design, the tradeoff is the anonymity protection degree and transmission delay. A larger number of hierarchies generate more routing hops, which increases anonymity degree but also increases the delay. To ensure the delivery of packets, the destination sends a confirmation to the source upon receiving the packets. If the source has not received the confirmation during a predefined time period, it will resend the packets.

proposed work

The major issue identified in ALERT, is that it cannot prevent strong active attacks like black hole attacks. In networking , black hole refers to places in network where incoming or outgoing traffic is silently discarded without informing the source that the data did not reach its destination. Black hole attack makes the nodes to refuse in participating in the network activities when an established node drops out. All network traffics are redirected to a specific node, which does not exist at all that causes those data to be lost. This may even lead to reveal its security concerns.

A black hole attack in ad hoc networks refers to an attack by malicious nodes, which forcibly acquire the route from the source to destination by falsely advertising to reach the destination node. The objective of the research work is to implement a well wisher routing protocol (WRP) and thereby to detect and prevent the black hole attacks.

Conclusion

MANET, a mobile ad hoc network is a self configuring infrastructure network of mobile devices connected by wireless .A routing protocol specifies how routers communicate with each other. The anonymous routing protocols rely either on redundant traffic or on hop-by-hop encryption, generating high cost. Some of the protocols are also unable to provide complete source, destination and route anonymity protection. ALERT is distinguished by lower cost and offering anonymity protection for sources, destinations and routers. ALERT is not completely bulletproof to all attacks.It cannot fight against blackhole attack which is a serious attack in MANETS.Thus the blackhole attack detection and prevention mechanism has to be included in ALERT.

REFERENCE

[1] 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. | [2] TOMASZ CISZKOWSKI AND ZBIGNIEW KOTULSKI "ANAP:ANONYMOUS AUTHENTICATION PROTOCOL IN MOBILE AD HOC NETWORKS ". | [3] G V ESWARA RAO, D.KAMAL KUMARI AND N.KRISHNA SANTHOSH,"CACS:CLOSED ANONYMOUS COMMUNICATION SYSTEM FOR MANENTS ". | [4] 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. | [5] 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. | [6] I. AAD, C. CASTELLUCCIA, AND J. HUBAUX, "PACKET CODING FOR STRONG ANONYMITY IN AD HOC NETWORKS," PROC. SECURECOMM AND WORKSHOPS, 2006. | [7] X. WU, "AO2P: AD HOC ON-DEMAND POSITION-BASED PRIVATE ROUTING PROTOCOL," IEEE TRANS. MOBILE COMPUTING, VOL. 4, NO. 4, PP. 335-348, JULY/AUG. 2005. | [8] Y. ZHANG, W. LIU, AND W. LUO, "ANONYMOUS COMMUNICATIONS IN MOBILE AD HOC NETWORKS," PROC. IEEE INFOCOM, 2005. | [9] 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. | [10] L. YANG, M. JAKOBSSON, AND S. WETZEL, "DISCOUNT ANONYMOUS ON DEMAND ROUTING FOR MOBILE AD HOC NETWORKS," PROC. SECURECOMM AND WORKSHOPS, 2006. | |