International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 7 331 – 336

Development of Advanced Location Based Efficient Routing in MANETs

Nair Swatichandra
Department of Information Technology
PIIT
Mumbai, India
swatichandrasekhar@gmail.com

Manjusha Deshmukh
Department of Computer Engineering
PIIT
Mumbai, India
mdeshmukh@mes.ac.in

Abstract—Mobile Ad Hoc Networks (MANETs) use routing protocols that are anonymous and provides hiding of crucial node identities and routes, so that outside observers cannot trace the route and also the crucial nodes, in this way it provides better protection. There are many existing anonymous routing protocols which rely on either hop-by-hop encryption or redundant traffic. Both the methods used are highly costly and also they don't generate full anonymity protection to the nodes or routers and also the source and destination. As the cost is high while using this anonymity protection categories it creates problem in the resource constraints in MANETs especially in multimedia wireless applications high cost exacerbates the intrinsic resource constraint problem are seen in MANETs especially in wireless multimedia applications. To provide protection at low cost, an Advanced Location-based Efficient Routing in MANET (ALER).It dynamically partitions the network field into different zones and it randomly chooses nodes in zones as intermediate relay nodes, these relay nodes forms a non-traceable anonymous route, not only that the proposed protocol also helps in hiding the sender and the destination also very efficiently. It also has strategies to effectively counter intersection, timing attacks. In this routing technique it has tried to overcome the Sybil attack issues which were not solved by the routing technique. It has prevented the Sybil attack entirely by having forwarding nodes check source routes for loops.

Keywords- *Advanced Location-based Efficient Routing in MANET (ALER),AODV,Sybil attack,NS2,Heirarchial partitton.*

*****

I. INTRODUCTION

A mobile adhoc networks can be called as groupof mobile users that convey through a bandwidth constrained wireless links. Here, node performs the duties such as finding the topology and delivering messages. A MANET can self-maintain itself, it is also responsible for forming by its own and it also heals by itself, due to these three properties much better flexibility is provided to the network by the MANETs. There is no base station required as the infrastructure is decentralized one. In MANETs each and every device is free to move in any direction independently, due to which it can easily change it link every now and then with other devices. Now a day's Mobile Ad Hoc Networks (MANETs) has gained lots of attention and popularity due to its use in numerous areas like education, military, emergency hospital needs,entertainment and commerce which has stimulated numerous wireless applications. MANET poses some major features life organizing itself and independent infrastructure for using in communication and sharing of information. Because of the decentralization feature of MANETs, the nodes can be a member or can detach itself from the network as the network is infrastructure less. Nodes in MANETs are vulnerable to malicious entities; there major aim is to tamper the original information provided and analyzing the confidential data by eavesdropping or by attacking the routing protocol.

In MANETs, the router connectivity may change frequently, leading to the multi-hop communication paradigm that can allow communication without the use of Base Station/Access Point, and provide alternative connections inside hotspot cells. A dual-mode MS can operate in both the infrastructure (communicating directly to a BS or AP) and Manet's modes using the WLAN interface. A MANETs is a type of ad hoc network that can change locations and configure itself on the fly. All nodes in this network are mobile and they use wireless connections to communicate with various networks. Routing is one of the core problems of networking for delivering data from one node to the other. Wireless adhoc networks are also called Mobile ad-hoc multihop networks without predetermined topology or central control. This is because MANETs can be characterized as having a dynamic, multihop, potentially rapid changing topology. A MANETs is usually formed by mobile nodes using wireless communications. It uses a peer-to-peer multihop routing instead of a static network infrastructure to provide network connectivity. The aim of such networks is to provide communication capabilities to areas with limited or no existing communication infrastructures.

The routing protocols in Adhoc networks are majorly divided into four main classes and they include proactive, reactive, hybrid protocol and position based routing protocols.In proactive routing, it stores routing information in order to maintain the routing information, to maintain the table and the changes occurred in the network topology. To maintain a consistent networking view it needs to update the whole time whenever any change is reflected by the network topology.

The conventional routing schemes an example is named as Destination sequenced distance vector (DSDV). Consistently attempts are made to up to-date routing information of the whole network. It determines which nodes are present or reachable in the network and due to which delay can be used in minimizing the delay occurred in the communication. Reactive routing is also known as on-demand routing protocol since they do not maintain any table that consists routing information or routing activity at the network nodes if there is no communication. If a node wants to send a data packet to another node then it tries to find a route by establishing the connection to transfer the data from sender node to the receiver or forwarder nodes. It has an on-demand feature. The Route request packets are flooded all over the network in order to discover a new route in the network. The major examples of reactive routing protocols are the Ad-hoc On-demand Distance Vector routing (AODV) and Dynamic Source Routing (DSR). A combination of reactive and proactive routing protocols is used to introduce a hybrid model. There is a hybrid protocol called as Zone Routing protocol which divides the network into several zones. Each and every node in the network has to maintain extra information about topology in order to provide additional memory; it also provides a hierarchical architecture. The individual nodes in the location based protocols assume that they are aware about the locations of all the nearby nodes present in the network. Global Positioning system is the best and most profound way to determine the coordinates exactly of these nodes in any geographical locations. The routes are determined by the routing protocol by utilizing the location information accumulated by Global Positioning System and few of the location based routing protocols are LAR, DREAM, GPSR, and LARDAR etc.The set of applications for MANET is diverse, ranging from large-scale, to small, mobile, to static, highly dynamic networks to that are constrained by power sources. Besides the legacy applications which moves from traditional infra structured environment into the adhoc context, a great number of new services are generated for the new environment.

Anonymity is very much important and critical in military applications (e.g., soldier communication) although it’s not required in civil oriented applications. Consider that there is a MANET deployed in a battlefield. Enemies can easily intercept the transmission of packets through traffic analysis by doing this they can easily track the positions of the soldiers (i.e. nodes), they can attack commander nodes and can easily block the data transmitted by comprising the relay nodes (RN). Anonymous routing protocols are crucial in MANETs to provide secure communications. The main goal of ALER is to provide identity and location anonymity of source and destination in MANET. For this ALER dynamically and randomly chooses relay node for forming route between source and destination. So due to this intruder cannot observe a statically pattern of transmission. Anonymous path between source and destination ensures that nodes on the path do not know where the end points are. Unlink ability is major strength of privacy protection i.e. source and destination cannot be associated with the packets in their communication by adversaries.There are mainly two anonymity routing techniques existing in MANETs the first one is hop-by-hop and the other one is redundant traffic. But both these method failed to provide complete anonymity protection. In order to which a new protocol came into existence and that is called as ALER, it is consider to give the maximum protection given to the sender and the destination nodes. To provide the network the at most protection it partitions the complete network into some zones and then it selects few random nodes which acts as intermediate relay nodes, which helps in forming an anonymous route, here in each routing step a data sender or forwarder partitions the network field in order to separate itself and the destination into two zones. Next step is to choose a node randomly from other zone which acts as the next relay node and the AODV algorithm is used to send the data packets forward. In the final step the data is transferred to 'k' number of nodes in the destination zone. Due to which it helps in providing anonymity in the destination zone.

II. RELATED WORK

Mobile Ad-hoc network is quick and it doesn't need any infrastructure to build a network. It mainly consist of wireless router's, nodes, etc. Mobile is random and perhaps its changing. It is the complete collection of many systems and interconnected hardware devices along with some communication channels this allows for sharing the information. Lot of researchers has done many effective works on MANET routing protocols. In this section we cite the relevant past literature that use the various protocols for routing in MANET and related work. The paper [4], author Karim El Defrawy and Gene Tsudik proposed some interesting issues arising in such MANETs by designing an anonymous routing framework (ALARM).here a map is produced using the location of nodes; based on this map the current node decides where it should forward the data. Here the ALARM protocol uses some cryptographic methods to provide the required authentication, anonymity, integrity of data and intractability. The paper [7], author B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, to provide more security and anonymity the requirements was increased so in order to provide the same a new protocol was emerged named as Anonymous Secure Routing (ASR) protocol this was emerged in order to overcome the disadvantages of ALARM protocol, it provided only weak location privacy whereas the ASR provides many anonymity properties which provide Strong authentication and location privacy gets stronger in order to which this protocol gets resilient to many vulnerable attacks. It also helps in making the discovered routes security stronger against the active and passive attacks. Xiaoxin Wu

and Bharat Bhargavaproposed [5]. An ad hoc on-demand position-based private routing algorithm, called AO2P, is proposed for communication anonymity. It was proposed for providing anonymity for the communication. It designed a scheme for receiver contention in order to determine the best next hop. It exposes the information i.e. the position information about the destination node. The real node identities are hidden and also the difficulty is in matching the actual identities from the actual global position and the real node identity. For making the match it uses a service system called the secure position service. To further improve destination privacy, R-AO2P is proposed. In this protocol, the position of a reference point, instead of the position of the destination, is used for route discovery.PriyankaGoyal, VintiParmar, Rahul Rishi has completed a complete survey on MANET's Vulnerabilities, challenges, Attacks, Application [3]. They have suggested all the possible vulnerabilities occurring in the MANET networks. They have also suggested some routing algorithms in order to improve the communication between the nodes. It discuss about some important characteristics of MANET like dynamic topology, scalability, availability of resource, etc. It also stated about certain security goals achieved .It has stated about many attacks possible, approaches of broadcasting, applications and challenges.

Zhi Zhou and Kin Choong Yow, proposed a new approach for the anonymous geographic routing algorithm [6], it contains mainly three components to vanish the exposure of location and identity, it hides the identity of the nodes communicating. This guarantees the protection about the entire network. The location of the nodes the route followed, are prevented due to which the location of the entire nodes and its path of routing is hidden.In this paper author provides the details about the prevention of nodes and it is mentioned as the model named k-anonymity [8] and for deploying a set of policies are accompanied. The release of k-1 individuals are not distinguished among the provided anonymity of k nodes,it also provides the details related to the information provided for every person. The entire information is maintained in the release.It also examines many attacks named as re-identification.It opens up the k-anonymity releases the polices that is accompanied.The basic real world system is implemented using this k-anonymity. The protection is provided privately to the entire information. An Anonymous Location-based Efficient Routing protocol (ALERT) [1].The network field is partitioned dynamically to form into different zones after this it chooses a random node in the zone and names it as an intermediate relay node. These nodes helps in forming a non-traceable route which also anonymous. It also provides secure network by hiding the initiators and receiver nodes. Thus, ALERT offers anonymity protection to sources, destinations, and routes. The attacks on timing and the intersection attacks are contradict effectively. The efficiency of anonymity is analyzed theoretically. Compared to the existing routing techniques, ALERT provides a better protection in the anonymity and cost is reduced drastically. Also, ALERT is much better option when compared to the GPSR geographical routing protocol. This paper [2] explores the attacks of depletion in the resource at the routing protocol layer, the entire network gets disabled due to node drainage and hence the power of the battery is becoming less. These attacks rely on popular protocol classes of routing; they are not dependent on specific protocols. All protocols are vulnerable to the Vampire attack which is unable to detect and are devastating to the entire network. This attack is very simple to inject the malicious node into the network. These malicious node gains all the battery power and it empty up the entire power and bandwidth. This paper provides the recovery or the mitigation methods to overcome these deadly types of attacks. The forwarding nodes are checked again if these nodes are used or not, in-order to avoid the duplication of nodes.

III. PROPOSED APPROACH ALER TO AVOID SYBIL ATTACK

For better understanding, let us assume the entire network area is generally a rectangle in which nodes are randomly distributed. 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 is provided to the node to locate the positions of nodes in the entire area for zone partitions in ALER.ALER provides a dynamic and unpredictable routing path thatconsists of a number of dynamically deter-mined intermediate relay nodes. A given area is horizontally partitioned into two zones A1 and A2. Then zone A1 is again vertically partitioned into zone B1 and B2. After that, B2 is further horizontally partitioned into two zones. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner. This partition process is called as hierarchical zone partition.ALER 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.

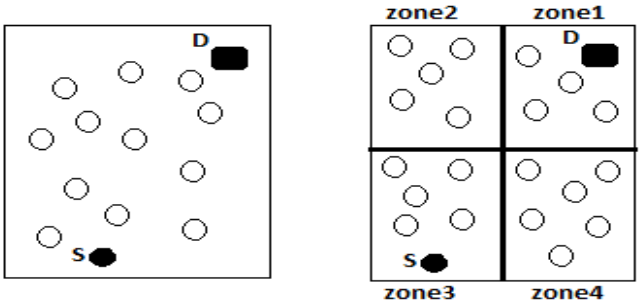

Figure 1: Partition of zones

Anonymous location based routing protocol implements the hierarchical zone partition that consists each and every data initiator or forwarder. It first checks whether the data initiator and destination are in the same zone or not. The zone gets divided into horizontal and vertical directions alternatively. Thisprocess is repeated until the source node itself and zone destination is not in the same zone. A node that is present in another zone is randomly selected and that node is called as temporary destination. The AODV routing algorithm is used to send the data to the node closest to the temporary destination. This node is defined as a random forwarder. Above figure 1 shows a flow for ALER. The first step is to create a MANET environment. Here, few nodes are taken and surmise that the entire network area is in rectangular in shape and nodes in it are randomly dispersed. The entire network area is divided into zones and selects a random forwarder. 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 vertical directions. The node repeats this process until itself and zone destinations are not in the same zone. It then randomly selects a position in the other zone called temporary destination, and uses AODV algorithm to send the data to the node that is closest temporary destination. The final zone contains number of nodes where it consists of final destination node, which is denoted as zone destination. The destination zone contains the final destination node.

The given system uses ALER technique in AODV routing protocols. Due to which it provides anonymity with the use of ALER technique. It also provides prevention from Sybil attack in order to avoid duplicate identities, energy consumption of nodes and reduction of network lifetime. In this strategy, MANET's takes the most important protocol AODV and apply it in the ALER routing technique for providing anonymity the route of packet forwarding cannot be determined and also location of the source and destination cannot be determined by the attacker. Thus using this strategy we can make AODV more secure. Here,AODV is used so as its nature is to broadcast the path request message to all the nodes in the network and from which node it receives the response it establishes the path with them and transfers the packet to them. But in the system it applies the ALER technique in AODV for anonymity protection, for this as in ALER it partitions the network into zones. But in this strategy it fix the zone partition value to four, means it partitions the network into four zones (zone1, zone2, zone3, and zone4). In very first step it divides the network into four zones (zone1, zone2, zone3, and zone4).A new variable is introduced in this strategy which is distance between each node, a value is fixed to a number (in this case it is 200). In the second step it finds that the neighbors of the source and destination are located in which zone out of four defined zone, for finding zone location in network to check for node in zone, the value is fixed in the upper left and lower right value of each zone. After finding each neighbor location in zones it calculates the distance of each neighbor from destination and finally selects those nodes which have distance value less than the fixed value (which is 200 in this case) as well as the node should fall in some region out of four regions. After the selection of nodes, a condition checks whether the nodes are already used or not, if the nodes are already used once again the ALER routing technique partitions the network and the procedure is repeated till the unused nodes are found. By doing this it is assured that there is no formation of loops. If a loop is detected then the packet send is drooped and the ALER routing technique partitions the zone again and whole procedure is followed again until the loop formation gets avoided. Then the source node multicast the packets to all neighbors of the destination and which neighbors have minimum distance value create the final path form source to destination.

A. Algorithm Stepsfor ALER

Step1: A rectangular network area is considered that consists of several nodes which are disseminated randomly in the entire network.

Step2: The hierarchical zone partition is accomplished by each data source or forwarder.

Step3: First it checks whether the source originator and the destination are in same zone.

Step4: Then it divides the zone using Hierarchical zone partition method.

Step5: Repeat step 4 process until source and zone destination are not in the same zone.

Step6: If source and zone destination are not in the same zone then it randomly selects a position in the other zone is called temporary destination.

Step 7: Check whether the nodes are already used or not.

Step8: AODV routing protocol is usedto send the data to the node closest to temporary destination. This node is defined as a random forwarder.

Step9: Repeat step 6 and step 7 until a data receiver finds itself residing in same zone destination that consists of knumber of nodes.

Step10: In the last step, the data is broadcasted to k number of nodes in the destination zone, providing k- anonymity to the destination node in order to hide it from the intruders.

B. Providing Privacy for ALER

In addition to that high privacy is provided inside the network. Two concepts are used and the first one is xoring method. This is used to reduce the overhead of the data packet transfers so hence it's an advantage and the node gets more network life. While merging the data packets, they are compressed into a smaller size compared to its original size. The advantage in doing so is that we are now able to two to three packets of data at once. A hash method is also used, it is a mathematical

 ISSN: 2321-8169
331 – 336

function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

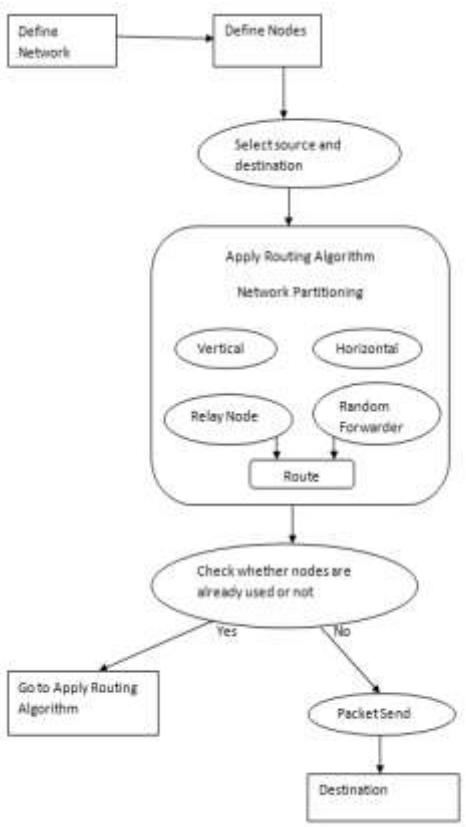

Figure 2: Architecture of Proposed System

C. Strategies Against Attacks

ALER offers identity and location anonymity of the source and destination, as well as route anonymity. Unlike geographic routing] which always takes the shortest path, ALER makes the route between a source and destination pair difficult to discover by randomly and dynamically selecting the relay nodes.It makes it difficult for an intruder to observe a statistical pattern of transmission occurring between the source and the receiver by providing different routes. The mechanisms called notify and go is incorporated by ALER, which prevents an intruder from identifying which node within the source neighborhood has initiated packets.ALER prevents an malicious node from interrupting the data packets or undermining any vulnerable nodes in the route. In ALER, it is difficult for the rivals to predict the route as the routes between two communicating nodes are constantly changing.

Using timing attacks intruders can identify the packets transmitted between the sender and the destination by using packet departure and arrival times. This results in finding out the sender and destination nodes. Avoiding the exhibition of interaction between communication nodes is a way to counter timing attacks [1].In ALER it uses two different mechanisms to cope up with this situation. The first one is called as notify and go mechanism and the second one is broadcasting in zone where destination is present. These are put in between the interaction of sender and destination into two sets of nodes to intruders.

In an intersection attack, an attacker keeps a track on the network from which information about active users can be accumulated at a given time. This fetches the details about the source and the destination nodes in the network.Intersection attacks are a well-known problem and have which can be solved by puzzling the attacker and lose the cumulated observation by making it occasionally fail to observe the destination receiving the packets.

There is one attack which is very dangerous and it is called Sybil attack, to interrupt the network it uses multiple identities or uses the identity of another node present in the network to communicate with the legitimate nodes in the network and to get the packet information. In order to avoid this attack we are using a technique where nodes are checked before participating in the network. The nodes are checked whether they are used before for the transmission of data packets. AODV uses destination sequence numbers to have loop free routes.

IV. CONCLUSION

Existing anonymous routing techniques either rely on hop-by-hop encryption or redundant traffic, both of them have a negative approach as it generate high cost. Not only that some of the existing protocols fail to provide complete protection to the network as some provide anonymity only to either source or destination nodes. Due to which complete protection of the network becomes a failure. But when a comparison is made between ALER technique and other existing ones,ALER is distinguished by others as it provides low cost and the anonymity protection is provided to the complete network from sender to the destination and also to the route the network follows. It uses a unique method of partitioning the zones in a dynamic hierarchical way which makes difficult to the outsiders to detect the route followed by the network and also the two end points i.e. the sender and the destination. ALER includes a packet rather than the position, which provides high protection in anonymity to the source and destination zones. ALER has characteristics to strengthen the anonymity by hiding the sender and the destination among a number of senders/receivers.The given system has also presented a novel approach on avoiding Sybil attack by having forwarding nodes check source routes for loops. This helps to avoid the Sybil attack and also reduce the network lifetime and energy consumption level of nodes. For the improvement of MANET there many possibilities and still many works are in progression phases.

REFERENCES

[1] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", Programmed random occurrence International Conference Parallel Processing (ICPP), 2013.

[2] Eugene Y. Vassermaand Nicholas Hopper Kansas State University University of Minnesota "Vampire attacks:Draining life from wireless ad-hoc sensor networks", Mobile (Volume: 12, Issue: 2),20 December 2012.

[3] PriyankaGoyal, VintiParmar, Rahul Rishi, "MANET: Vulnerabilities, challenges, Attacks, Application", International Journal of Computational Engineering &Management IJCEM, Vol. 11, January 2011.

[4] K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", Programmed random occurrence IEEE International Conference Network Protocols (ICNP), 2009.

[5] 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.

[6] 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.

[7] K. El-Khatib, L. Korba, R. Song, and G. Yee, "Anonymous Secure Routing in Mobile Ad-Hoc Networks",Programmed random occurrence International ConferenceParallel Processing Workshops (ICPPW), 2003.

[8] L. Sweeney, "k-Anonymity: A Model for Protecting Privacy", International Journal Uncertainity Fuzziness Knowledge-Based Systems, vol. 10, no. 5,pp. 557-570, 2002.