Volume 6, Issue 1, January 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Alternate Path Approach to Avoid Intrusion Detection

Rajesh Rajaan, Dinesh Sharma
Department of Computer Science
India

Abstract—Mobile ad hoc networks (MANETs) consist of a collection of wireless mobile nodes in a continuously self-configuring, infrastructure less network or a wired backbone network. The ad-hoc network provides lack of secure boundaries. The meaning of this vulnerability is self-evident: there is not such a clear secure boundary in the mobile ad hoc network, which can be compared with the clear line of defence in the traditional wired network. There are some issues in the design of MANETs. These are small range, diverse, static constraints that are power sources, to large scale, mobile, highly dynamic networks. Today the intruder attack in an ad hoc network is increasing very fast. To avoid this attack algorithmic implementation is done to transfer the data over the network. For secure communication we need to provide maximum efficiency and maximum security to the ad hoc networks. For this purpose we generally use the shortest path algorithm, but there are many problems arises due to less security and less efficiency with this algorithm, like intruder attack and centralized load. We are working to search an Intruder Safe path that is not shortest but closer to the shortest.

Keywords—Path Intrusion Safe, Secure, Preventive, Predictive, MANET

I. INTRODUCTION

In the ad hoc networks there is no access points for passing information between participants and it act as LAN. LAN is a network can be built by connecting devices spontaneously. In MANETs communication between nodes is done through the wireless medium. Because nodes are mobile and may join or leave the network at any time, MANETs have a dynamic topology. The nodes which are used for transferring data are called neighbors because they are in the transmission range. So they can send data directly to each other. When a node send his data to another node which is not neighbor then a route is generated through a sequence of multiple hops, by maintaining shortest path i.e. minimum no. of nodes also known as routers.

A. Unicast Routing in MANET

In unipath routing, as the name suggest in this only a single route is used between a source and destination node for transferring data. To find and maintain route between source and destination nodes routing protocols are used. Two main classes of ad hoc routing protocols are table-based and on-demand protocols [4]:

- Table Based Protocols: Each node maintains a routing table containing routes to all nodes in the network. In this Nodes periodically exchange messages with routing information to keep routing tables up-to-date. Therefore, routes between nodes are computed and stored, even when they are not needed.
- On Demand Protocols: Nodes only compute routes when they are needed. Therefore On-demand protocols consist of the following two main phases:

1. Route discovery is the process of finding a route between two nodes.
2. Route maintenance is the process of repairing a broken route or finding a new route in the presence of a route failure.

There are two widely used protocols named as Dynamic Source Routing (DSR) and AODV and DSR are both on-demand protocols [5] [6] both are on demand protocols.

Dynamic Source Routing- DSR was developed at CMU in 1996.in this route discovery cycle is used for finding the route (on demand). In this no periodic activity was found. And maintenance is active in this process. In this entire route is the part of the header. Caches are used to store the route. Like any source routing protocol, in DSR the source includes the full route in the packets' header. The intermediate nodes are used to forward this packet to the destination nodes and the intermediate nodes maintain a route cache to follow the route.

Route discovery- If the source does not have a route to the destination in its route cache, it broadcasts a route request (RREQ) message specifying the destination node for which the route is requested. The RREQ message includes a route record which specifies the sequence of nodes traversed by the message.

1) The node is the Target (Destination)

Returns a Route Reply (RREP) message to the sender.

- Copies the accumulated route record from RREQ into RREP
- Sender upon receiving RREP, caches the route in its route cache for subsequent routing.

2) The node is the intermediate node.
   1. The node discards this message, if
   a). The message has the same ID i.e. has seen it before.
   OR
   b). Finds its own address in the route record
   - If Not, The node appends its own address to the route record in the ROUTE REQUEST message
   a). Propagates the message to the next hop neighbors.

Like when an intermediate node receives a RREQ, it checks to see if it is already in the route record. If it is, it drops the message. This is done to prevent routing loops. If the intermediate node had received the RREQ before, then it also drops the message. The intermediate node forwards the RREQ to the next hop according to the route specified in the header. When the destination receives the RREQ, it sends back a route reply message. If the destination has a route to the source in its route cache, then it can send a route response (RREP) message along this route.

Route maintenance- When a node detects a broken link while trying to forward a packet to the next hop, it sends a route error (RERR) message back to the source containing the link in error. When an RERR message is received, all routes containing the link in error are deleted at that node.

Ad Hoc On Demand Distance vector- AODV is an on-demand routing protocol for ad hoc networks. AODV uses hop-by-hop routing by maintaining routing table entries at intermediate nodes. There are many request type defined in AODV, like Route Requests (RREQs), Route Replies (RREPs) and Route Errors (RERRs. These message types are received via UDP and normal IP header processing applies. So, for instance the requesting node is expected to use its IP address as the Originator IP address for the messages.

Route Discovery- Route discovery is a process for a host in the ad hoc network to discover a route to deliver a packet to any other host. To initiate route discovery, the source floods the network with a RREQ packet containing the address of the destination for which the route is requested. When a node receives an RREQ packet, it checks to see whether it is the destination or whether it has a route to the destination. If either case is true, the node generates an RREP packet, which is sent back to the source along the reverse path. We set a forward pointer for all the node in reverse path for which the node receive the RREP. This sets up a forward path from the source to the destination. If the node is not the destination and does not have a route to the destination, it rebroadcasts the RREQ packet. When the source node receives the first RREP, it can begin sending data to the destination.

Route Maintenance- Route maintenance is done by means of route error (RERR) packets. When an intermediate node detects a link failure (via a link-layer feedback, e.g.), it generates a RERR packet. The RERR propagates towards all traffic sources having a route via the failed link, and erases all broken routes on the way. A source upon receiving the RERR initiates a new route discovery if it still needs the route. Apart from this route maintenance mechanism, AODV also has a timer-based mechanism to purge stale routes.

In this a table is maintained which fields are as follows-

- Destination IP address
- Destination Sequence Number
- Valid Destination Sequence Number Flag
- Other state and routing flags
- Network Interface
- Hop Count (needed to reach destination)
- Next Hop
- Precursor List

B. Multipath Routing in MANET

Our objective in this section is to extend the AODV protocol to compute multiple disjoint loop-free paths in a route discovery. We assume that every node has a unique identifier (UID) (e.g., IP address), a typical assumption with ad hoc routing protocols. For simplicity, we also assume that all links are bidirectional, that is, a link exists between a node i to j if and only if there is a link from j to i. AOMDV can be applied even in the presence of unidirectional links with additional techniques to help discover bidirectional paths.Standard routing protocols in ad hoc wireless networks, such as AODV and DSR, are mainly intended to discover a single route between a source and destination node. Multipath routing consists of finding multiple routes between a source and destination node.

I) Route Discovery and Maintenance- AOMDV also finds routes on demand using a route discovery procedure. The main difference lies in the number of routes found in each route discovery. In AOMDV, RREQ propagation from the source towards the destination establishes multiple reverse paths both at intermediate nodes as well as the destination. Multiple RREPs traverse these reverse paths back to form multiple forward paths to the destination at the source and intermediate nodes. Note that AOMDV also provides intermediate nodes with alternate paths as they are found to be useful in reducing route discovery frequency. Multipath routing protocols can attempt to find node disjoint, link disjoint, or non-disjoint routes. Node disjoint routes, also known as totally disjoint routes, have no nodes or links in common. Link disjoint routes have no links in common, but may have nodes in common. Non-disjoint routes can have nodes and links in common. From a fault tolerance perspective, more reliable paths should be selected to reduce the chance of routes failures. Path selection also plays an important role for QoS routing. In QoS routing, only a subset of paths that together satisfies the QoS requirement is selected.

C. Split Multipath Routing

Split Multipath Routing (SMR) proposed is an on-demand multipath source routing protocol. SMR is similar to DSR, and is used to construct maximally disjoint paths. Unlike DSR, intermediate nodes do not need to keep a route cache, and therefore, do not reply to RREQs. In this all paths are checked by from source to destination node and find the maximally disjoints paths. Because maximally disjoints paths have fewer links or nodes in common as possible. Duplicate routes do not need to discard.

Security Issues in Manet

There is no centralized manager for the adhoc network to manage the data, when the data is transmitted over the adhoc. Due to this Intruder attach are increases. These attacks can be occur in uni path or multi path routing. The Intruder attack is on the algorithmic approach of data transfer. Some of the common attacks on security are:-

I) Spoofed, Altered, or Replayed Routing Information This is the most direct attack against a routing protocol. Adversaries may be able to create routing loops, extend or shorten source routes, generate false error messages, partition the network, or increase end-to-end delay latency

II) Selective Forwarding: Malicious nodes may refuse to forward certain messages, drop them, ensuring that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a *black hole* and it refuses to forward every packet she sees. It is most effective when the attacker is explicitly included on the path of a data flow.

II. EXISTING WORK

According to a standard approach of communication between 2 nodes it is always based on the shortest path. The shortest path give no of benefits like Easy implementation, Fast and reliable data transfer between nodes. One of the common algorithm for selecting the path is given below

Path(A,n)

/* A is the Weighted graph of n size to represent the Adhoc Network*/

{

Step 1: Generate the neigbor list for the source node and put it in the matrix.

Step 2: Starting from the first neighbor generate the next neighbor.

Step 3: check if that neighbor already exist in the list if yes than it is a loopback and goto end;

Step 4: Generate the route from all the neighbors for the destination and continue on that path.

Step 5: Generate the route to destination from all neighbors where ever possible.

Step 6: Compare the route length generated by all the possible routes. Compare all the routes in the distance matrix and choose the path to destination which has the lowest path length.

}

This approach of data transfer is very common in case of dynamic topology like the sensor network. But as the intruder attacks according to the same approach it gives the very high chances of Data hack. In this diagram, there are number of possible paths and as a reliable and fastest path, the client will always select the shortest path .But this approach has some problems based on security and reliability. some are as follows:

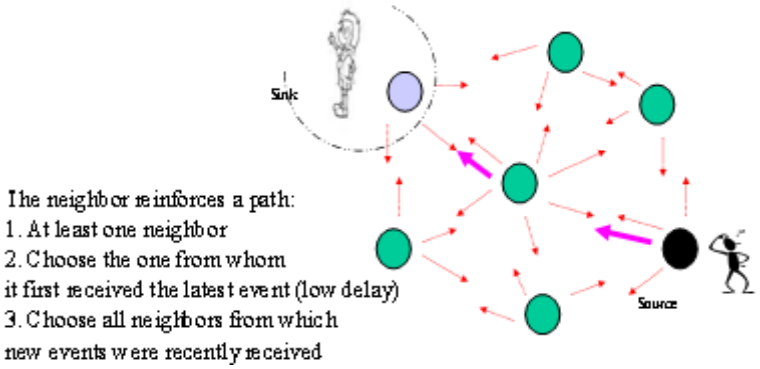

Fig. 1 Traditional Routing

1. Select One Shortest path

- Use of wireless links in shortest path susceptible to link attacks
- Relatively poor protection as in Battlefields.
- Passive eavesdropping
- Attacks from compromised attacks.

2. MultiPath

- Flooding: As an incoming packet is sent on all incoming links,it limit the number of hops to avoid infinite loops or forward packets only once using a packet ID or only on selected links in the right direction
- Multicasting: Terribly expensive in terms of resource utilization and results in minimum delay

We are suggesting the alternate path approach that is close to the shortest path and more reliable and secure. Security Requirements of Ad-Hoc Network Security Requirements of Ad-Hoc Network are:

- Route signalling can't be spoofed
- Fabricated routing messages can't be injected into the network
- Routing messages can't be altered in transit
- Routing loops can't be formed by through malicious action
- Routes can't be redirected from the shortest path by malicious action
- Unauthorized nodes should be excluded from route computation and discovery.

III. PROPOSED WORK

In this section, we present our mechanism (Secure Data Transmission using alternate Path in Ad hoc Network). At every round the network establishes a new routing topology by setting up new alternate routing paths. When we find the alternate path, we have to fulfill the following constraints:

(a) maximum path length(MaxLen)

MaxLen represents the maximum acceptable length of a path defined as the sum of edge weights *wi* in the path. The path length may represent various physical properties, such as distance, cost, delay, or failure probability. It can be represented by i an integer or a float value. If *wi* = 1 is true for all edges, then the path length is the hop number from a source to a destination.

(b) maximum number of hops on the path *(MaxHop)*

MaxHop represents the maximum acceptable number of hops on a path. If a path contains *k* nodes, then its hop number is *k-1*. *MaxHop* is an integer value.

(c) maximum number of shared edges *(MaxSE)*

Shared edges among three paths, also called common edges, include two types of edge sharing: double- and triple-shared edges, respectiv ely. We use integer values *MaxSEdbl* and *MaxSEtri* to denote the related maximum acceptable number of double- and triple-shared edges. This constraint is essential in cases requiring high network reliability when multiple paths are used between two routers.

PathAtoB (A,n.a.n)

/* A is the Adjacency matrix representation of Given network, n is the no of nodes and a,b are two nodes between we have to transfer data*/

{

Step 1:- Give the range of the network node and set all other elements that are outside the range to 0.

Step 2:- Find the Neighbor of Each node of network starting from node a to node b.

Step 3:- Find the shortest path from source to destination and store it in an array called array[].

Step 4:- Search the neighbor list and pick a random node from the list and put that node in the array.

Step 5:- compare the random node with all the elements of the shortest path array. If the array[top] element matches with any of the elements in the list then Make the entry corresponding to that node in neighbor array.

Step 6:- Compare the neighbor list of the generated node with all the elements of array otherwise Pick a random node from the list and put it in the array

}

Finally we get the list of nodes that provide a safe path in case of unicast, this pass is very closer to the shortest path but doest not include any node from the shortest path list because of this it provide the secure transmission on the algorithm implementation attack of the Intruder.

IV. CONCLUSION

Importance of MANET cannot be denied as the world of computing is getting portable and compact. Unlike wired networks, MANET pose a number of challenges to security solutions due to their unpredictable topology, wireless shared medium, heterogeneous resources and stringent resource constraints etc. The Security research area is still open as many of the provided solutions are designed keeping a limited size scenario and limited kind of attacks and vulnerabilities. We are providing the solution for the problems where we can save the adhoc network from the active attack of Intruders that are on the basis of algorithmic implementations. Generally the path selected for data transfer in adhoc network is the shortest path because of this intruder attack is also in same area. We have generated such a path in which no node from the shortest path will be included. It will give a secure and efficient approach of data transmission in adhoc network in unicast.

REFERENCES

[1] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci ,"*A Survey on Sensor Networks*", in Proc. of the IEEE Communications Magazine, vol.40, Issue: 8, pp. 102-114, Aug. 2002.

[2] Qiangfeng Jiang and D. Manivannan,"*Routing Protocols for Sensor Networks*", in Proc. of the IEEE Conference, 2004, pp. 93-98.

[3] Nam N. Pham, Jon Youn and Chulho Won,"*A Comparison of Wireless Sensor Network Routing Protocols on an Experimental Testbed",* in Proc. Of the IEEE International Conference on Sensor Networks, 2006, pp.35-42

[4] Chris Karlof and David Wagner,*"Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures"*, University of California at Berkeley, Tech. Rep. F33615-01-C-1895.

[5] A.Perrig, R.Szewczyk, V.Wen and J.D. Tygar, "SPINS*: Security Protocols for sensor networks*", International Conference on Mobile Computing and Networking (Mobicom 2001), 2001, pp.189-199.

[6] A.D. Wood and J.A. Stankovic, "*Denial of service in sensor networks",* IEEE Computer 35 (10), 2002, pp. 54-62.

[7] Lewis, F.L.,*"Wireless Sensor Networks Smart Environments: Technologies, Protocols, and Applications"*, New York: ed. D.J. Cook and S.K. Das, John Wiley, 2004, pp.1-18.

[8] J. Deng, R. Han and S. Mishra, "*INSENS: Intrusion-Tolerant Routing in WSN",* in Proc. Of the Second International Workshop on Information Processing in Sensor Networks (IPSN 03), April 2003, pp. 349-364.

[9] Dijkstra E. *A note on two problems in connection with graphs*. Numerical Mathematics 1959; 1:269-271.

[10] T. Korkmaz, M. Krunz, and S. Tragoudas, *"An efficient algorithm for finding a path subject to two additive constraints"*, in Proceedings of the ACM SIGMETRICS '00 Conference, June 2000, vol. 1, pp. 318–327.

[11] Thierry Rakotoarivelo , Patrick Senac , Aruna Seneviratne and Michel Diaz, *"Enhancing QoS through Alternate Path: An End-to-End Framework"*, in Proc. of the IEEE INFOCOM, Conference on Computer Communications, pp. 14-22, 2000.

[12] Dr. Sami S. ,Al-Wakeel and Eng. Saad A. AL-Swailem , "*PRSA: A Path Redundancy Based Security Algorithm for Wireless Sensor Networks*", in Proc. of the IEEE Communications Society, pp. 4159-4163, 2007.

[13] Wei Wang, Sylvani Gombault, "*Efficient Detection of DDoS Attack with Important Attributes*", 3rd International Conference on Risks and Security of Internet and System: CRiSIS' 2008, IEEE, 2008.

[14] Yinan Jing, Xueping Wang, Xiaochun Xiao, Gendu Zhang,*"A Logless Fast IP Traceback Scheme Against DDos Attacks in wireless Ad-hoc Network"*

