An Alternative Path Analysis and Routing in Mobile Ad-hoc Network

Isha Nagpal
Jagannath University, Jaipur, India
isha_nagpal2008@yahoo.com

Abstract — Mobile Ad hoc network consists of a set of mobile nodes and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. Mobile Ad Hoc Network (MANET) may consist of hops through other hosts in the network. Therefore, the task of finding and maintaining routes in MANET is nontrivial. Mobile ad-hoc network does not have any infrastructure or central administration, hence it is called infrastructure less network. This paper presents an alternative path between nodes in mobile ad hoc network. We generally choose the shortest path to transmit the data which is not safe due to the probability of attack of the intruder. There are number of intrusion detection and prevention technique to overcome with different types of attacks. An alternate path scheme provides a security oriented approach for designing the routing protocol Mobile Ad-hoc networks. It proposes the new cluster based security architecture which starts from the initialization of the network.

Keywords — Alternative path analysis, MANET, mobile ad-hoc network, Routing algorithm

I. INTRODUCTION

Mobile Ad hoc network is self configuring network of mobile hosts connected by wireless links, the union of which forms the topology of the network [1]. The advantages of ad hoc networks are the convenience (no central administration), mobility, productivity and expandability. As the nodes in the network are mobile, the topology of network changes unpredictably. A mobile ad hoc network (MANET) sometimes called a mobile mesh network, comprised of mobile computing devices (nodes) that use wireless transmission for communication and do not rely on any central coordinator. Mobile nodes that are within each other’s radio range communicate directly via wireless links, while those far apart rely on other nodes to relay messages as routers. These tiny sensor nodes communicate with each other using low power wireless data routing protocols such as Directed Diffusion, PEGASIS [2], Multi Hop Router, GF (Greedy Forwarding) [3] etc. This paper deals with an alternative path analysis and finding the best alternative path in communication link. According to this, a group of mobile agents builds path between pairs of nodes by exchanging information and updating routing tables. Routing protocols for Mobile Ad Hoc Networks generate a large amount of control traffic when node mobility causes link states and the network topology to change frequently. Mobility can be of two types. In the waypoint mobility model, each node chooses a random target which is uniformly distributed in the surface and advances towards it at a constant velocity. When it reaches the target, a new target is generated and the node moves again. In the random walk model, nodes move at each step in one of the four cardinal directions, and reflect at the boundary.

In other words, wireless sensor network generally consists of a data distribution network and data acquisition network monitored and controlled by a management center as shown in Fig.1 with the center having the responsibility of providing secure distribution over the network. But sometimes the management center fails to provide the desired security which motivates the researchers to design new secure and effective routing algorithms for data packet routing.

The sensor network consists of a base station or gateway that can communicate with a number of wireless sensors via a radio link as shown in fig. 2.

Data is collected at these sensor nodes where it is compressed and transmitted to the gateway directly or via...
other intermediate sensor nodes i.e. sensor network supports multi hop communications. For the secure transmission of this aggregated data to sink node, secure routing scheme becomes a great necessity.

A. Attacks on mobile Networks

Attack can be of any type i.e. it can be outsider attack or insider attack. In the former case, an outside entity or attacker cannot have special access to the sensor network. In case of insider attack, a legitimate node has been compromised and has unwanted effects on the network. This kind of attack is hard to determine or we can say, more severe as compared to outsider attack. Most network layer attacks against mobile ad-hoc networks fall into one of the following categories [4].

- Wormholes: Adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part.
- Spoofered, altered routing attack: Adversary makes efforts to replay routing information, create routing loops, and to extend or shorten source routes. It tries to become what it is not i.e. it befools the legitimate nodes.
- Sinkhole attacks: Adversaries make the compromised node look attractive to surrounding nodes with respect to the routing choice and creates a metaphorical sinkhole.
- Sybil attacks: Type of attack in which a single node presents multiple identities to other nodes in the network.
- Acknowledgement spoofing: An adversary can spoof link layer acknowledgments for “overheard packets” addressed to neighboring nodes.
- Selective forwarding: Adversaries refuse to forward certain messages, to simply drop them, and to attract or repel network traffic.

II. EXISTING ROUTING TECHNIQUE

When intruder want to hack some information by acting man in middle, it is not easy for him to trace all the nodes over the network because the sensor network contains large number of nodes. In such case instead of tracking each node, intruder follows a route or the pattern to perform the attack. One of such method is to trace the shortest path. Generally each routing algorithm follows the concept of shortest path to transfer the data over the network with minimum time requirement. In other words we can say shortest path route nodes are the most unsafe nodes for transferring data as they are generally targeted by the intruder. In order to route the data immediately i.e. without much delay, nodes follow a greedy approach i.e. shortest path.

The problem to compute this shortest path has been provided with so many solutions in the literature. Various algorithms designed to solve this shortest path problem includes Dijkstra's algorithm [9] which solves the single-pair, single-source, and single-destination shortest path problems, Bellman-Ford algorithm [10] which solves the single source problem if edge weights may be negative, Floyd-Warshall algorithm [11] which solves all pairs shortest paths etc.

Routing scheme given by Dijkstra's involves an algorithm which is a graph search algorithm that solves the single-source shortest path problem for a graph with nonnegative edge path costs, producing a shortest path tree. This algorithm is often used to compute the shortest cost effective route towards the destination node for the purpose of routing data over wireless sensor networks. For a given source vertex (node) in the graph, the algorithm finds the path with lowest cost (i.e. the shortest path) between that vertex and every other vertex as shown in fig 3. It can also be used for finding costs of shortest paths from a single vertex to a single destination vertex by stopping the algorithm once the shortest path to the destination vertex has been determined.

Fig. 3 Shortest path graph problem

In uni-path routing, only a single route is used between a source and destination node. The Protocols which are used in routing are helpful in finding and maintaining routes between source and destination nodes.

Two types of classes of ad hoc routing protocols are table-based and on-demand protocols:

1) Proactive Protocols: Proactive routing protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network by propagating, proactively, route updates at fixed intervals. As the resulting information is usually maintained in tables, the protocols are sometimes referred to as table-driven protocols.

2) On Demand Protocols: Nodes only compute routes when they are needed. On-demand protocols consist of the following two main phases:

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

Two of the widely used protocols are Dynamic Source Routing (DSR) and the Ad hoc On-demand Distance Vector (AODV) protocols. AODV and DSR are both on-demand protocols.

3) Dynamic Source Routing: The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network.

• Route Discovery: It checks whether it has the valid route entry in its cache. If no, broadcasts a route request packet. Each intermediate node checks whether it knows of a route to the destination; route records is placed in the reply message.

“Route request” packet contains a route record yielding the sequence of hops taken. “Route reply” is generated when the request reaches the either the destination or an intermediate node that has a valid route to the destination; route records is placed in the reply message.

Route Maintenance - When a node detects a broken link while attempting 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.

4) Ad Hoc on Demand Distance vector: It is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. In contrast, the most common routing protocols of the Internet are proactive, meaning they find routing paths independently of the usage of the paths. AODV is, as the name indicates, a distance-vector routing protocol. AODV avoids the counting-to-infinity problem of other distance-vector protocols by using sequence numbers on route updates, a technique pioneered by DSDV. AODV is capable of both unicast and multicast routing.

• Route Discovery: The route discovery process is initiated when a source needs a route to a destination and it does not have a route in its routing table. To initiate route discovery, the source floods the network with a RREQ packet specifying 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. When the source node receives the first RREP, it can begin sending data to the destination.

• Route Maintenance: When a node detects a broken link while attempting to forward a packet to the next hop, it generates a RERR packet that is sent to all sources using the broken link. The RERR packet erases all routes using the link along the way. If a source receives a RERR packet and a route to the destination is still required, it initiates a new route discovery process.

III. ALTERNATE PATH ANALYSIS AND ROUTING

In this section, we present our mechanism (Data Transmission using alternate Path in mobile 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-shared and triple-shared edges, respectively. We use integer values MaxSEdbl and MaxSEtri to denote the related Path A to B(A.n.a.n)

IV. ALGORITHM

/* 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 an 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.

Step 7: Find the problematic node in the path, if any exclude from the list.

Finally, we get the list of nodes that provide a safe path in case of uni-cast, this pass is very close to the shortest path but does 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. The algorithm does not assumes a predefined network topology i.e. network is initialized first and then the maximum amount of data to be sent over the network or we can simply say data packet size as well as maximum elapsed time for defining network lifetime has to be stated. All the constraints defined in the above section have to be taken into account before applying the proposed algorithmic scheme.

V. CONCLUSION

Shortest path is used to transmit sensory data over the sensor networks. The existing algorithm for finding this shortest path was given by Dijkstra which is not a safe data transmission technique. As the shortest path is more prone to intruder attack, an alternate path which is secure from intruder attack would be developed because intruder would be interested in shortest path, it won’t be having any information about its existence. If any of these conditions are met, then the alternate path would be followed for data transmission. If there a node failure or if there is congestion on the existing shortest path or if the shortest path is no longer secure.

Thus, a secure alternate path would be established for routing sensory data over wireless sensor network. If some other unsafe node exists, then it can also be removed from data transmission path. It means the direct attack on a known node can also be handled.

REFERENCES


