An Alternative Path Routing Scheme for Intrusion Prevention in Wireless Network
Parveen Yadav, Harish Saini

Abstract - An ad hoc network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnection between nodes are capable of changing on a continual basis. The recent progress and advances in computing and communication technologies have led to the development of the concept of mobile computing. The unique characteristics of mobile ad hoc networks create a number of security threats to the development of it. We generally choose the shortest path to transmit the data which is not safe due to the probability of attack of the intruder. Even when the Intruder knows about the routing algorithms or the algorithm implementation it is quite difficult to handle the problem. In this paper, we are providing the approach to transfer data from some path other than that common path. There are number of intrusion detection and prevention methods to deal with different types of attacks. Our alternate path scheme provides a security oriented approach for designing the routing protocol of wireless sensor networks. It proposes the new cluster based security architecture which starts from the initialization of the network. Safe path is not shortest but next alternative shortest path in mobile ad hoc network.

Keywords - Mobile Ad hoc Network, WSN, AODV, Intrusion Detection.

I. INTRODUCTION

Wireless Sensor networks (WSN) can be defined as the network of geographically distributed tiny sensor nodes, which have sensing, computing and wireless communicating capabilities [1]. This new approach is a type of wireless networking, which is comprised on number of numerous sensors. Sensors are interlinked or connected with each other for performing the same function collectively or cooperatively for the sake of checking and balancing the environmental factors.

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. Sensor networks are increasingly becoming important in real world application areas, ranging from critical military applications to monitoring of building security. Ad hoc networks are subjected to various kinds of attacks. In wireless network communication links can be eavesdropped on without noticeable effort and communication protocols on all layers are vulnerable to specific attacks. In contrast to wire-line networks, known attacks like masquerading, man-in-the-middle, and replaying of messages can easily be carried out. To deploy sensor networks in such applications, security is an unavoidable aspect and should be provided against various attacks such as node capture [4], physical capture [4], denial of service [6] etc.

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.

Fig.1 Wireless Sensor Network Composition [7]

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.

2. Spoofed, 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.

3. Sinkhole Attacks: Adversaries make the compromised
node look attractive to surrounding nodes with respect to the
routing choice and creates a metaphorical sinkhole.

4. Sybil Attacks: Type of attack in which a single node
presents multiple identities to other nodes in the network.

5. Acknowledgement Spoofing: An adversary can spoof
link layer acknowledgments for “overheard packets”
addressed to neighboring nodes.

6. Selective Forwarding: Adversaries refuse to forward
certain messages, to simply drop them, and to attract or repel
network traffic.

II. EXISTING ROUTING SCHEME

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,
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.
Route discovery is the process of finding a route between source and destination nodes. 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:

(a) **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.

(b) **On Demand Protocols**: Nodes only compute routes when they are needed. 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.

### 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. 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. PROPOSED ALGORITHM (Secure Alternate Path)

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-shared and triple-shared edges, respectively. We use integer values MaxSEdbl and MaxSEtri to denote the related path Atob(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 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.

Finally, we get the list of nodes that provide a safe path in case of uni-cast, this pass is very closer 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 assume 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 elaphed 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.

**IV. CONCLUSION**

The 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 intruder safe and easily fall prey to intruder attack. 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**


