EFFICIENT IMPLEMENTATION OF DYNAMIC ROUTING WITH SECURITY CONSIDERATIONS

UMADEVI DURVASULA¹, A KIRAN KUMAR²

¹Department of Information Technology, Aditya Institute of Technology and Management, Tekkali, Andhra Pradesh, India. Email: umadevi.durvasula1@gmail.com
²Assistant Professor, Department of Information Technology, Aditya Institute of Technology and Management, Tekkali, Andhra Pradesh, India.

Abstract—Now-a-days security is one of the major issues for data communication over wireless and wired networks. The past work on the designs of cryptography algorithms and system infrastructures, Apart from that the authors proposed a dynamic routing algorithm called improved dynamic routing with security consideration, which is based on the concept of Zone Routing Protocol (ZRP) that could randomize delivery paths for data transmission. The algorithm is easy to implement and compatible with popular routing protocols, such as the Routing Information Protocol (RIP) in wired networks and Destination-Sequenced Distance Vector (DSDV) protocol in wireless networks, without introducing extra control messages. This improves security as well as controls traffic in the network. A clear study on the proposed algorithm is presented, and a series of simulation experiments are conducted to verify the results and to show the capability of the proposed algorithm.

Index Terms— Dynamic Routing, ZRP, DSDV, RIP.

I. INTRODUCTION

An ad hoc network is a collection of wireless computers(nodes), communicating among themselves over possibly multi-hop paths, without the help of any infrastructure are popularly such as base stations or access points[1,2]. Unlike conventional mobile wireless networks, ad hoc networks greatly improve having no fixed infrastructure. 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. In ad hoc network each node acts both as a host (which is capable of sending and receiving) and a router which forwards the data intended for some other node. Applications of ad hoc network range from military operations and crisis disaster relief, to commercial uses such as community networking and interaction between attendees at a meeting or students during a lecture. Most of these applications demand a secure and reliable communication. The objective of this work is to explore a security enhanced routing algorithm based on distributed routing information widely supported in existing wired and wireless networks. We aim at the randomization of delivery paths for data transmission to provide considerably small path similarity (i.e., the number of common links between two delivery paths) of two consecutive transmitted packets. These protocols shall not increase the number of control messages if the proposed algorithm is adopted. An analytic study will be presented for the proposed routing algorithm, and a series of simulation study will be conducted to verify the analytic results and to show the capability of the proposed algorithm.

In this paper, we proposed a secure hybrid ad hoc routing protocol, called Hybrid broadcast Routing with Security Consideration, which takes the advantage of both proactive and reactive approach. Our proposed protocol is based on zone routing protocol (ZRP) [3,4]. The reasons for selecting ZRP as the basis of our protocol are as follows: (i) ZRP is based on the concept of routing zones, a restricted area, and it is more feasible to apply the security mechanisms within a restricted area than in a broader area that of the whole network, (ii)Since the concept of zones separate the communicating nodes in terms of interior (nodes within the zone) and exterior (nodes outside the zone) nodes, certain information like network topology and neighborhood information etc. can be hidden to the exterior nodes, (iii) In case of a failure, it can be restricted within a zone. We will use a dynamic routing algorithm to provide security enhanced data delivery without introducing any extra control messages.

II. LITERATURE SURVEY

A. Data transmission

Data transmission, digital transmission or digital communications is the physical transfer of data (a digital bit stream) over a point-to-point or point-to-multipoint transmission medium. Examples of such media are copper wires, optical fibers, wireless communication media, and storage media. The data is often represented as an electro-magnetic signal, such as an electrical voltage signal, a radio wave or microwave signal or an infra-red signal[5,6]. While analog communications represents a continuously varying signal, a digital transmission
can be broken down into discrete messages. The messages are either represented by a sequence of pulses by means of a line code (base band transmission), or by a limited set of analogue wave forms (pass band transmission), using a digital modulation method. According to the most common definition of digital signal, both baseband and pass band signals representing bit-streams are considered as digital transmission, while an alternative definition only considers the baseband signal as digital, and the pass band transmission as a form of digital-to-analog conversion.

Data transmitted may be digital messages originating from a data source, for example a computer or a keyboard. It may also be an analog signal such as a phone call or a video signal, digitized into a bit-stream for example using pulse-code modulation (PCM) or more advanced source coding (data compression) schemes. This source coding and decoding is carried out by codec equipment[7,8].

B. Adaptive routing

Adaptive routing describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in conditions. The adaptation is intended to allow as many routes as possible to remain valid (that is, have destinations that can be reached) in response to the change.

People using a transport system can display adaptive routing. For example, if a local railway station is closed, people can alight from a train at a different station and use another method, such as a bus, to reach their destination.

The term is commonly used in data networking to describe the capability of a network to 'route around' damage, such as loss of a node or a connection between nodes, so long as other path choices are available. There are several protocols used to achieve this:

- RIP
- OSPF

Systems that do not implement adaptive routing are described as using static routing, where routes through a network are described by fixed paths (statically). A change, such as the loss of a node, or loss of a connection between nodes, is not compensated for. This means that anything that wishes to take an affected path will either have to wait for the failure to be repaired before restarting its journey, or will have to fail to reach its destination and give up the journey.

C. Routing Information Protocol

The Routing Information Protocol (RIP) is a dynamic routing protocol used in local and wide area networks. As such it is classified as an interior gateway protocol (IGP). It uses the distance-vector routing algorithm. It was first defined in RFC 1058 (1988). The protocol has since been extended several times, resulting in RIP Version 2 (RFC 2453). Both versions are still in use today, however, they are considered technically obsolete by more advanced techniques, Open Shortest Path First (OSPF) and the OSI protocol IS-IS. RIP has also been adapted for use in IPv6 networks, a standard known as RIPng.

D. Destination-Sequenced Distance Vector routing

Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad hoc mobile networks based on the Bellman-Ford algorithm. It was developed by C. Perkins and P.Bhagwat in 1994. The main contribution of the algorithm was to solve the Routing Loop problem. Each entry in the routing table contains a sequence number, the sequence numbers are generally even if a link is present; else, an odd number is used. The number is generated by the destination, and the emitter needs to send out the next update with this number. Routing information is distributed between nodes by sending full dumps infrequently and smaller incremental updates more frequently[8,9].

E. Selection of Route

If a router receives new information, then it uses the latest sequence number. If the sequence number is the same as the one already in the table, the route with the better metric is used. Stale entries are those entries that have not been updated for a while. Such entries as well as the routes using those nodes as next hops are deleted.

i. Advantages

DSDV was one of the early algorithms available. It is quite suitable for creating ad hoc networks with small number of nodes. Since no formal specification of this algorithm is present there is no commercial implementation of this algorithm. Many improved forms of this algorithm have been suggested.

F. Multipath routing

Current routing schemes typically focus on discovering a single "optimal" path for routing, according to some desired metric. Accordingly, traffic is always routed over a single path, which often results in substantial waste of network resources. Multipath Routing is an alternative approach that distributes the traffic among several "good paths instead of routing all traffic along a single "best" path.

Equal-cost multi-path (ECMP) is a routing technique for routing packets along multiple paths of equal cost. The forwarding engine identifies paths by next-hop. When forwarding a packet the router must decide which next-hop (path) to use[9,10].
**G. Zone Routing Protocol**

The Zone Routing Protocol (ZRP) [3, 4] was introduced in 1997 by Haas and Pearlman. It is either a proactive or reactive protocol. It is a hybrid routing protocol. It combines the advantages from proactive (for example AODV) and reactive routing (OLSR). It takes the advantage of pro-active discovery within a node’s local neighbourhood (Intrazone Routing Protocol (IARP)), and using a reactive protocol for communication between these neighbourhoods (Interzone Routing Protocol (IERP)). The Broadcast Resolution Protocol (BRP) is responsible for the forwarding of a route request. It shown in the Fig 1.

ZRP divides its network in different zones. That's the nodes local neighbourhood. Each node may be within multiple overlapping zones, and each zone may be of a different size. The size of a zone is not determined by geographical measurement. It is given by a radius of length, where the number of hops is the perimeter of the zone. Each node has its own zone. radius=2-Hop E, D, B, J, E and H are border-nodes.

![Fig 1 Zone Routing Protocol](image)

Before constructing a zone and determine border nodes, a node needs to know about its local neighbours. A node may use the media access control (MAC) protocols to learn about its direct neighbours. It also may require a Neighbour Discovery Protocol (NDP). ZRP does not strictly specify the protocol used but allows for local independent implementations. NDP relies on the transmission of hello messages by each node. When the node for example node A gets a response from a node B which has received the "Hello"-message, the node A notice that it has a direct point-to-point connection with that node B.

**III. Problem Analysis**

**A. Problem Statement**

On the other hand, the discovery of paths in an offline fashion might not be suitable to networks with a dynamic changing configuration. Therefore, we will propose a dynamic routing algorithm to provide security enhanced data delivery without introducing any extra control messages. The objective of this work is to explore a security enhanced dynamic routing algorithm based on distributed routing information widely supported in existing wired and wireless networks. We aim at the randomization of delivery paths for data transmission to provide considerably small path similarity (i.e., the number of common links between two delivery paths) of two consecutive transmitted packets.

**B. Hybrid Broadcast Routing With Security Considerations**

**i. Notations and Data Structures**

The objective of this section is to propose a hybrid broadcast routing algorithm to improve the security of data transmission. The hybrid Routing with security consideration Protocol is based on zone routing protocol (ZRP) [3,4]. Like ZRP it Performs intra zone and inter zone routing; however, it differs from ZRP in security aspects. In ZRP where there is no security consideration, hybrid broadcast routing with security Consideration designed to address all measure security concerns like end to end authentication, message/packet integrity and data confidentiality during both intra and inter-zone routing. For end to end authentication and message integrity RSA digital signature mechanism [11] is employed, where as data confidentiality is ensured by an integrated approach of both symmetric and asymmetric key encryption [11]. Each communicating node has two pairs of private/public keys, one pair for signing and verifying and the other for encrypting and decrypting.

We propose to rely on existing information exchanged among neighbouring nodes (referred to as routers as well in this paper) for the seeking of routing paths. In ZRP each node Ni maintains a routing table (see Table 1a) in which each entry is associated with a tuple (t, WNi, Nexthop), where t, WNi, and Nexthop denote some unique destination node, an estimated minimal cost to send a packet to t, and the next node along the minimal-cost path to the destination node, respectively. With the objective of this work in the randomization of routing paths, the routing table shown in Table 1a is extended to accommodate our security-enhanced dynamic routing algorithm. In the extended routing table (see Table 1b), we propose to associate each entry with a tuple(t, WNi,t,Ct,WNi,Ht) Ct,WNi is a set of node candidates for the next hop (note that the candidate...
selection will be elaborated in Procedure 2 of Section 3.2), where one of the next hop candidates that have the minimal cost is marked. \( H_i^N \), a set of tuples, records the history for packet deliveries through the node \( N_i \) to the destination node \( t \). Each tuple \((N_j, h_{N_j}) \) in \( H_i^N \) is used to represent that \( N_i \) previously used the node \( h_{N_j} \) as the next hop to forward the packet from the source node \( N_j \) to the destination node \( t \). Let \( N_{br}\) and \( w_{Ni,Nj} \) denote the set of neighboring nodes for a node \( N_i \) and the cost in the delivery of a packet between \( N_i \) and a neighbouring node \( N_j \), respectively. Each node \( N_i \) also maintains an array (referred to as a link table) in which each entry corresponds to a neighbouring node \( N_j \in N_{br} \) and contains the cost for a packet delivery \( w_{Ni,Nj} \).

The proposed algorithm achieves considerably small path similarity for packet deliveries between a source node and the corresponding destination node. However, the total space requirement would increase to store some extra routing information. The size of a routing table depends on the topology and the node number of a network under discussions. In the worst case, we have a fully connected network. For each entry in the routing table shown in Table 1b, the additional spaces required for recording the set of node candidates (as shown in the third column of Table 1b) and for recording the routing history (as shown in the fourth column of Table 1b) are \( O(|N|) \). Because there are \( |N| \) destination nodes at most in each routing table, the additionally required spaces for the entire routing table for one node are \( O(|N|^2) \).

Since the provided distributed dynamic routing algorithm (HBRA) is a distance-vector-based routing protocol for intra domain systems, the number of nodes is limited, and the network topology is hardly fully connected. Hence, the increase of the total space requirement is considerably small. However, the impact of the space requirement on the search time will be analysed in the following section[12,13].

<table>
<thead>
<tr>
<th>Destination Node(t)</th>
<th>Cost( (W_{Ni,t}) )</th>
<th>Nexthop</th>
<th>History Record for Packet Deliveries to TheDestination Node t (( H_i^N ))</th>
</tr>
</thead>
<tbody>
<tr>
<td>( N_1 )</td>
<td>9</td>
<td>( N_6 )</td>
<td>{ (( N_2 ), ( N_3 )), (( N_1 ), ( N_3 )), ..., (( N_{31} ), ( N_{20} )) }</td>
</tr>
<tr>
<td>( N_2 )</td>
<td>10</td>
<td>( N_{21} )</td>
<td>{ (( N_1 ), ( N_0 )), (( N_3 ), ( N_0 )), ..., (( N_{31} ), ( N_{21} )) }</td>
</tr>
<tr>
<td>( N_3 )</td>
<td>11</td>
<td>( N_9 )</td>
<td>{ (( N_1 ), ( N_0 )), (( N_2 ), ( N_0 )), ..., (( N_{31} ), ( N_9 )) }</td>
</tr>
</tbody>
</table>

Table 1 a) The routing table for the original distance-vector-based routing algorithm

Table 1 b) The routing table for the proposed security enhanced routing Algorithm

**C. Hybrid Broadcast Routing With Security Consideration Algorithm**

The HBRA proposed in this paper consists of two parts:

1) A randomization process for packet deliveries and
2) Maintenance of the extended routing table.

**D. Randomization Process**

Consider the delivery of a packet with the destination \( t \) at a node \( N_i \). In order to minimize the probability that packets are eavesdropped over a specific link, a randomization process for packet deliveries shown in Procedure 1 is adopted. In this process, the previous nexthop \( h_s \) (defined in of Table 1b) for the source node \( s \) is identified in the first step of the process (line 1). Then, the process randomly picks up a neighbouring node in excluding \( h_s \) as the next hop for the current packet transmission. The exclusion of \( h_s \) for the nexthop selection avoids transmitting two consecutive packets in the same link, and the randomized pickup prevents attackers from easily predicting routing paths for the coming transmitted packets.

**Procedure 1 RANDOMIZED SELECTOR (s, t, pkt)**

1: Let \( h_s \) be the used nexthop for the delivery for the source node \( s \).
2: if \( h_s \in C_i^N \) then
3: if \( |C_i^N| > 1 \) then
4: Randomly choose a node \( x \) from \( C_i^N\) - \( h_s \) as a nexthop, and send the packet \( pkt \) to the node \( x \).
5: \( h_s \leftarrow x \), and update the routing table of \( N_i \).
6: else
7: Send the packet pkt to h,
8: end if
9: else
10: Randomly choose a node y from $C_t^{Ni}$ as a nexthop, and send the packet pkt to the node y.
11: $h_i ← y$, and update the routing table of $N_i$.
12: end if

E. Routing Table Maintenance

Let every node in the network be given a routing table and a link table. We assume that the link table of each node is constructed by an existing link discovery protocol, such as the Hello protocol. On the other hand, the construction and maintenance of routing tables are revised based on the well-known Bellman-Ford algorithm [14] and described as shown in Fig 2:

![Fig 2 Distributed dynamic routing algorithm](image)

**DVPROCESS**($t,W_{Ni,t}$)

1: if the destination node $t$ is not in the routing table then
2: Add the entry ($t,(W_{Ni,Nj}+W_{Nj}), C_i^{Ni} = \{Nj\}; H^{Ni}_t = \emptyset$)
3: else if ($W_{Ni,Nj}+W_{Nj,t} < W_{Ni,t}$) then
4: $C^{Ni}_t ← \{Nj\}$ and $Nj$ is marked as the minimal-cost nexthop.
5: $W_{Ni,t} ← (W_{Ni,Nj}+W_{Nj,t})$
6: for each node $N_k ≠ Nbr_i$ except $Nj$ do
7: if $W_{Nk,t} < W_{Ni,t}$ then
8: $C^{Ni}_t ← C^{Ni}_t U \{Nk\}$
9: end if
10: end for
11: Send ($t,W_{Ni,t}$) to each neighboring node $N_k ∈ Nbr_i$.
12: else if ($W_{Ni,Nj}+W_{Nj,t} > W_{Ni,t}$) then
13: if ($Nj ∈ C^{Ni}_t$) then
14: if $Nj$ was marked as the minimal-cost nexthop then
15: $W_{Ni,t} ← \text{MIN}_{Nk ∈ Nbr_i} (W_{Nk,Ni} + W_{Nk,t})$
16: $C^{Ni}_t ← \emptyset$
17: for each node $N_k ∈ Nbr_i$ do
Initially, the routing table of each node (e.g., the node $N_i$) consists of entries $\{(N_j, w_{N_i,N_j}, C_{N_j}^{N_i} = \{N_j\}, H_{N_j}^{N_i} = \emptyset)\}$, where $N_j \in \text{Nbr}_i$ and $w_{N_i,N_j} = w_{N_j,N_i}$. By exchanging distance vectors between neighboring nodes, the routing table of $N_i$ is accordingly updated. Note that the exchanging for distance vectors among neighboring nodes can be based on a predefined interval. The exchanging can also be triggered by the change of link cost or the failure of the link/node. In this paper, we consider cases when $N_i$ receives a distance vector from a neighboring node $N_j$. Each element of a distance vector received from a neighboring node $N_j$ includes a destination node $t$ and a delivery cost $w_{N_j,t}$.

IV. TEST CASES

To spot all the structural, syntactical and integration errors in the code, a series of test cases are prepared and the application was tested rigorously using these cases. The system passed most of these, and in case of any discrepancy from the expected behavior, that portion of the module was immediately modified to make it error free.

The test cases used to evaluate the system are given below:

1. Test Case: When a link/node failure is occurred.
   Expected Result: When a link/node failure is occurred, the data packets are transmitted by using the backup route.
   Observed Result: Same as expected result.

2. Test Case: When a link/node failure is recovered.
   Expected Result: When a link/node failure is recovered, the data packets are transmitted by using the backup route.
Expected Result: When a link/node failure is recovered, the data packets are transmitted by using the original route.
Observed Result: Same as expected result.

The simulation of Secure Hybrid broadcast Routing Protocol was conducted in NS-allinone-2.34, on an Intel core i3 processor and 1 GB of RAM running Ubuntu 10.0 Lts.

A. Network topology

In the proposed Network scenario, we simulated two types of field configurations: 50 nodes distributed over a 700m x 700m terrain and 50 nodes over a 1200m x 1200m terrain. Node transmission range was taken to be 250m. The initial positions of the nodes were random. Node mobility was simulated according to the random waypoint mobility model, in which each node travels to a randomly selected location at a configured speed and then pauses for a configured pause time, before choosing another random location and repeating the same steps. We ran simulations for a constant node speeds of 0, 1, 5... and 10 m/s, with pause time fixed at 30 seconds.

B. Simulation Results and Analysis

In this section we present and analyse the observed results for each of the performance metric discussed in the previous section under the network and security setup. The resulting data were plotted using Gnu plot. Each data point in the resulting graphs is an average of simulations runs with identical configuration but different randomly generated mobility patterns. To compare the performances of the protocols, the following metrics are used. Packet delivery ratio: The ratio of the data packets successfully delivered at destination.

i. Average Packet Delivery ratio

Figure 5 below shows the observed results for average packet delivery fraction for both the networks. As shown in the figure, the packet delivery fraction obtained using Hybrid Routing with Security Consideration (HBRA) is above 96% in all scenarios and almost identical or higher than that obtained using ZRP. This suggests that HBRA is highly effective in discovering and maintaining routes for delivery of data packets, even with relatively high node
Effect of Traffic Load on Throughput

This section elaborates on the effect of traffic load on throughput for ZRP, and our HBRA. Note that since the performance of HBRA with Randomized Selector the curve for HBRP_without Randomized Selector will not be plotted. Figs. 6 show the experimental results of the throughput under different traffic loads for HBRA_with Randomized Selector, ZRP, and From these figures, we can observe that the throughput would be degraded when the number of TCP flows increases (i.e., the traffic load increases). Furthermore, for all values of traffic loads under investigation, the performance of HARA_with RandomizedSelector on the throughput is superior as compared with that of ZRP.

Average single-trip time

Fig 7. Show the experimental results of the average single-trip time under the proposed HBRA, ZRP.

VI. CONCLUSIONS AND FUTURE WORK

The simulation results for Hybrid broadcast Routing with Security Consideration under different mobility patterns and traffic scenarios show that the proposed protocol is as efficient as ZRP in discovering and maintaining routes. However, the impact of the overhead caused is almost insignificant and negligible as compared to the proposed degree of security, which provides compared to its other counterparts.

The advantages of a multipath approach are clearly exemplified. We can conclude that the multipath approach can increase confidentiality.

References


