ISSN:0975-9646

Hybrid Broadcast Routing with Dynamic Security Considerations

S.Ramasubba Reddy[#], O. Srinivasa Rao[#], Dr MHM Krishna Prasad[*]

[#]Dept of CSE, UCEV_JNTUK
Vizianagaram, AP, India

[*]Dept of IT, UCEV_JNTUK
Vizianagaram, AP, India

Abstract— **An ad hoc network is the supportive engagement of a collection of mobile nodes without the required interference of any centralized access point or existing infrastructure. There is an increasing trend to adopt ad hoc networking for profitable uses; however, their main applications lie down in military, strategic and other security-sensitive operations. In these and other applications of ad hoc networking, secure routing is an important issue. Most of the secure routing protocols proposed in the literature are either proactive or reactive in nature. In this paper, we proposed for ad hoc network, called hybrid broadcast routing with security consideration, which is based on the concept of Zone routing protocol (ZRP).Different from the past work on the designs of cryptography algorithms and system infrastructures, we will propose a dynamic routing algorithm that could randomize delivery paths for data transmission. The algorithm is easy to implement and well-suited with popular routing protocols, without introducing extra control messages. An analytic study on the proposed algorithm is presented, and a series of simulation in wireless networks, experiments are conducted to verify the analytic results and to show the capability of the proposed algorithm.**

Keywords— **Security-enhanced data transmission, dynamic routing, Ad-hoc Routing protocols, RIP, NS-2.**

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 have 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) [13],[14]. 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 neighbourhood 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

The rest of this paper is organized as follows: Section 3 discuss about the related work. Section 3 formally defines the Problem under investigation. In Section 4, we propose a hybrid broadcast routing with security consideration algorithm to randomize the data delivery paths. An analytic study on the proposed algorithm is conducted. Section 5 summarizes our experimental results to demonstrate the capability of the proposed algorithm. Section 6 is the conclusion

II. Related work

Today, Internet security has become an important issue. Many companies try to incorporate commerce in the Internet to give its customers more flexibility. To incorporate commerce business in the Internet we have to make it more secure and more trusted. So Internet securities have become a major research topic today. Many techniques have been developed to cover this hole in the Internet.

Among many well-known designs for cryptography-based systems, the IP Security (IPSec) [12] and the Secure Socket Layer (SSL) supported and implemented in many systems and platforms. Though IPSec and SSL do the security level for data transmission, they unavoidably introduce substantial overheads

Especially on gateway/ host performance and effective network bandwidth. Another alternative for security-enhanced data transmission is to dynamically route packets between each source and its destination so that the chance for system break-in, due to successful interception of consecutive packets for a session, is slim. The intention of security-enhanced routing is different from the adopting of multiple paths between a source and a destination to increase the throughput of data transmission (see, e.g., [5] and [6]). In particular, Lou et al.[10],[12],[7] proposed a secure routing protocol to improve the security of end-to-end data transmission based on multiple path deliveries. The set of multiple paths between each source and its destination is determined in an online fashion, and extra control message exchanging is needed. Bo hacek et al. [2] [7] proposed a secure stochastic routing mechanism to improve routing security. Similar to the work proposed by Lou et al. [10], a set of paths is discovered for each source and its destination in an online fashion based on message flooding. Thus, a mass of control messages is needed. Yang and Papavassiliou explored the trading of the security level and the traffic dispersion. They proposed a traffic dispersion scheme to reduce the probability of eavesdropped information along the used paths provided that the set of data delivery paths is discovered in advance. Although excellent research results have been proposed for security-enhanced dynamic routing, many of them rely on the discovery of multiple paths either in an online or offline fashion. For those online path searching approaches, the discovery of multiple paths involves a significant number of control signals over the Internet. On the other hand, the discovery of paths in an offline fashion might not be suitable to networks with a dynamic changing configuration.

III. THESIS OBJECTIVE

The objective of this work is to explore a security–enhanced Hybrid broadcast routing Algorithm based on distributed Routing information widely supported in existing networks. In general, routing protocols over networks could be classified roughly into two kinds: distance-vector algorithms and link- state algorithms [8]. Distance-vector algorithms rely on the exchanging of distance information among neighbouring nodes for the seeking of routing paths. Examples of distance-vector-based routing algorithms include RIP and DSDV. Link-state algorithms used in the Open Shortest Path First protocol are for global routing in which the network topology is known by all nodes. Our goal is to propose a distance-vector-based algorithm for dynamic routing to improve the security of data transmission. Before we proceed with further discussions, our problem and system model shall be defined.

A network could be modelled as a graph G= (N, L), where N is a set of routers (also referred to as nodes) in the network, and L is a set of links that connect adjacent routers in the network. A path p from a node s (referred to as a source node) to another node t (referred to as a destination node) is a set of links (N1,N2) (N2,N3)…(NI,NI+1),where S=Ni,Ni+1=t,Nj∊N, and (NJ,Ni+1)∊L for 1≤ j≤ i .Let Ps,t denote the set of all potential paths between a source node s and a destination node t. Note that the number of paths in Ps,t could be an exponential function of the number of routers in the network, and we should not derive Ps,t in practice for routing or analysis.

A. *Definition 1(path similarity)*

Given two paths pi and pj, the path similarity Sim (pi, pj) for pi and pj is defined as the number of common links between pi and pj: Sim (pi, pj)=│{(Nx,Ny) │ (Nx,Ny) ϵ pi ^(Nx,Ny) ϵpj}│, where Nx and Ny are two nodes in the network. The path similarity.

B. *Definition 2 (the expected value of path similarity for any two consecutive delivered packets).*

Given a source node s and a destination node t, the expected value of path similarity of any two consecutive delivered packets is defined as follows:

E[Sim s,t]=∑ sim(pi,pj) . prob(pj│ pi.Prob(pi),
∀pi, pjϵ Ps, t

Where Ps, t is the set of all possible transmission paths between a source node s and a destination node t. Prob (pi│ pj) is the conditional probability of using pj for delivering the current packet, given that pi is used for the previous packet. Probo ((pi), is the probability of using pi for delivering the previous packet. Between two paths is computed based on the algorithm of Levenshtein distance.

IV. HYBRID BROADCAST ROUTING WITH SECURITY CONSIDERATIONS

A. 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) [13], [14]. 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,t, Nexthop), where t, WNi, t, 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,C_t^{Ni},H_t^{Ni}) C_t^{Ni} is a set of node candidates for the next hop (note that the candidate selection will be elabo-rated in Procedure 2 of Section

3.2), where one of the next hop candidates that have the minimal cost is marked. H_t^{Ni} a set of tuples, records the history for packet deliveries through the node Ni to the destination node t. Each tuple (Nj,h_{Nj})in H_t^{Ni} is used to represent that N_i previously used the node h_{Nj} as the nexthop to forward the packet from the source node Nj to the destination node t. Let Nbri and wNi,Nj denote the set of neighboring nodes for a node Ni and the cost in the delivery of a packet between Ni and a neighbouring node Nj, respectively. Each node Ni also maintains an array (referred to as a link table) in which each entry corresponds to a neighbouring node Nj Є Nbri and contains the cost for a packet wNi,Nj delivery. 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 discus- sions. 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.

Destination Node(t)	Cost($W_{Ni,t}$)	Nexthop
N_1	9	N_6
N_2	10	N_{21}
N_3	11	N_9
:	:	:

Fig a) The routing table for the original distance-vector-based routing algorithm.

Destination Node(t)	Cost ($w_{Ni,t}$)	Nexthop Candidates (C_t^{Ni})	History Record for Packet Deliveries to The Destination Node t(H_t^{Ni})
N_1	9	{ N_6, N_{21}, N_9}	{(N_2, N_{21}),(N_3, N_6),…,(N_{31}, N_{20})}
N_2	10	{ N_9, N_{21}}	{(N_1, N_9),(N_3, N_9),…,(N_{31}, N_{21})}
N_3	11	{ N_9}	{(N_1, N_9),(N_2, N_9),…,(N_{31}, N_9)}
:	:	:	:

Fig b) The routing table for the proposed security enhanced routing Algorithm.

B. 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.

1) Randomization Process

Consider the delivery of a packet with the destination t at a node Ni. 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 hs(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 nexthop for the current packet transmission. The exclusion of h_s for the nexthop selection avoids transmit- ting 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 hs be the used nexthop for the delivery for the source node s.
2: if hs Є $C_t^{Ni}$ then
  3: if | $C_t^{Ni}$ |> 1 then
    4: Randomly choose a node x from { $C_t^{Ni}$ -hs } as a nexthop, and send the packet pkt to the node x.
    5: $h_s$ ← x, and update the routing table of Ni.
  6: else
    7: Send the packet pkt to $h_s$.
  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: $h_s$ ← y, and update the routing table of $N_i$.
12: end if
```

2) 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 [4] and described as follows:

Initially, the routing table of each node (e.g., the node N_i) consists of entries {(N_j, wN_i,N_j , C_{Nj}^{Ni} ={Nj}, H_{Nj}^{Ni} =ø},where N_j Є Nbr_i and wN_i,N_j = wN_i,N_j. By exchanging distance vectors between neighbouring nodes, the routing table of Ni is accordingly updated. Note that the exchanging for distance vectors among neighbouring 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 Ni receives a distance vector from a neighbouring node N_j. Each element of a distance vector received from a neighbouring node N_j includes a destination node t and a delivery cost WN_j; t from the node N_j to the destination node t. The algorithm for the maintenance of the routing table of Ni is shown in Procedure 2, which is adopted from [4].

V. SIMULATION ENVIRONMENT

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 Ubuntu10.0 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.

1) Average Packet Delivery ratio

Figure 1 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.

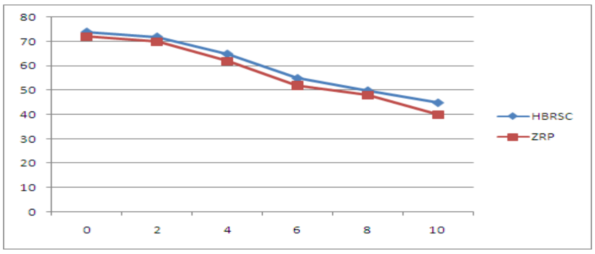

Figure 1.Delivery ratio of HBRA and ZRP in a scenario of 50 nodes, in this graph, x-axis represents the speed (m/s) and y-axis represents the packet delivery ratio.

2) 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. 2 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.

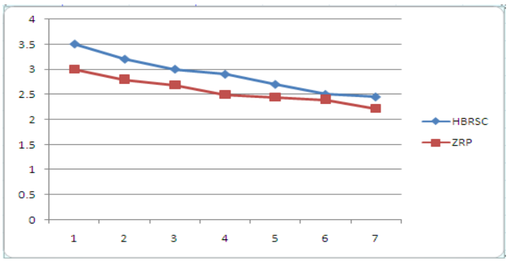

Figure 2. In this graph, x-axis represents the TCP flows and y-axis represents the throughput per flow

3) Average single-trip time

Fig 3. Show the experimental results of the average single-trip time under the proposed HBRA, ZRP. These figures indicate that the HBRA does not result in much longer single-trip-time compared with ZRP

In this graph, x-axis represents the length of the minimal-cost path and y-axis represents the single-trip time.

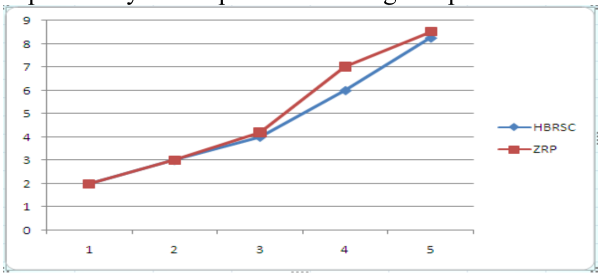

Fig 3) Single Triptime

VI. CONCLUSION

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

[1] C. Siva Ram Murthy and B. S Manoj, "AdHoc Wireless Networks, Architecture and Protocols", Prentice Hall PTR, 2004.

[2] Stefano Basagni, Macro Conti, Silvia Giordano andIvan Stojmenovic, "Mobile Ad Hoc Networks", IEEE press, A john Wily & Sons, INC. publication, 2003.

[3] George Aggelou,"Mobile Ad Hoc Networks", 2nd edition, Mc GRAW Hill professional engineering,2004.

[4] T.H. Cormen, C.E. Leiserson, and R.L. Rivest, Introduction to Algorithms. MIT Press, 1990.

[5] I. Gojmerac, T. Ziegler, F. Ricciato, and P. Reichl, "Adaptive Multipath Routing for Dynamic Traffic Engineering," Proc. IEEE Global Telecommunications Conf. (GLOBECOM), 2003.

[6] C. Hopps, Analysis of an Equal-Cost Multi-Path Algorithm, Request for comments (RFC 2992), Nov. 2000.

[7] C. Kaufman, R. Perlman, and M. Speciner, Network Security—PRIVATE Communication in a PUBLIC World, second ed. Prentice Hall PTR, 2002.

[8] J.F. Kurose and K.W. Ross, Computer Networking— A Top-Down Approach Featuring the Internet. Addison Wesley, 2003.[10] V.I. Levenshtein, "Binary Codes Capable of Correcting Deletions,Insertions, and Reversals," Soviet Physics Doklady, vol. 10, no. 8,pp. 707-710, 1966.

[9] S.-H. Liu, Y.-F. Lu, C.-F. Kuo, A.-C. Pang, and T.-W. Kuo, "The Performance Evaluation of a Dynamic Configuration Method over IPSEC," Proc. 24th IEEE Real- Time Systems Symp.: Works in Progress Session (RTSS WIP), 2003.

[10] W. Lou and Y. Fang, "A Multipath Routing Approach for Secure Data Delivery," Proc. IEEE Military Comm. Conf. (MilCom), 2001.[12] W. Lou, W. Liu, and Y. Fang, "SPREAD: Improving Network Security by Multipath Routing," Proc. IEEE Military Comm. Conf. (MilCom),2003.

[11] M. O. Pervaiz, M. Cardei, and J. Wu, "Routing Security in Ad Hoc Wireless Networks," Network Security, S. Huang, D. MacCallum, and D. -Z. Du (eds.), Springer,2008.

[12] R. Thayer, N. Doraswamy, and R. Glenn, IP Security Document Roadmap, Request for comments (RFC 2411), Nov. 1998.

[13] Haas Z. J., Pearlman M. R., and Samar P., "The Zone Routing Protocol(ZRP)",IETF Internet Draft, draft-ietf-manet-zone-zrp-04.txt, July 2002.

[14] Jan Schaumann, "Analysis of Zone Routing Protocol", Course CS765, Stevens Institute of Technology Hoboken, New Jersey, USA, 8th December 2002.