ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Advanced Randomized Security Algorithm for Internet and Wireless Networks

Kondapalli Beulah
Department of CSE,
GVP College of Engineering,
Visakhapatnam.

Penmetsa V Krishna Raja
Department of CSE,
Sri Vatsavai Krishnam Raju
College of Engineering &
Technology, Bhimavaram.

Gudikandhula Narasimha Rao
Dept. of Geo Engineering &
Centre for Remote Sensing,
Andhra University College of
Engineering, Visakhapatnam,
Andhra Pradesh, India.

Abstract:

Security has become one of the major issues for data trans¬fer over wired and wireless networks in real world. Smart society is becoming more dependent on various communication networks such as the Internet and the sensor networks. These networks need strong security measures to keep the traffic secure. If the security fails, many aspects of the society may suffer. In this paper, we address the network security challenge by focusing on one integral part of the network functionality dynamic routing. The proposed system introduced Advanced Open Shortest Path First (AOSPF) with Internal Gateway Protocol (IGP). It creates a randomization process in which the packets will be sent through less predictable paths. By using this process we expect to increase the difficulty for a hacker to eavesdrop traffic hence improve network security. So even if the routing algorithm becomes known to the adversary, the adversary still can¬not find out all the routes traversed by each packet. The experimental results clearly show the great advantages of the naive routing algorithm for small-scale wireless networks and Internet.

Index Terms:

Internet security, routing algorithm, AOSPF, path randomization, Classification.

1. INTRODUCTION:

Dynamic Routing is one of the fundamental functionalities of various communication networks such as the Internet and the sensor networks. Routers, and more broadly, switches are the backbone of the communication networks, thus making them a prime target for malicious attacks [1]. Current technology like Secure Socket Layer (SSL) and IP Security (IPSec) provide a decent level of security to network applications but at the cost of efficiency [2] [3].

The routing process is dictated by protocols which define what a router should do when a packet arrives. Some of these protocols have built-in security measures to ensure the authenticity of the message. For example, the Open-Shortest- -Path-First (OSPF) protocol has a simple password protection and cryptographic authentication [4] [6]. In addition to the lack of message confidentiality, OSPF also does not protect against sniffing software which has the ability to intercept Link State Advertisement messages and learn the whole network topology. OSPF uses a shortest path algorithm such as Dijkstra's algorithm to find the shortest or lowest cost path from the source router to the receiving router [5] [7]. This ensures each data package will be sent most efficiently through the network. A major weakness of this approach is that if an attacker were to know the topology of the network, he/she could easily predict the exact path by which each message will be sent as long as the network topology is relatively stable [8].

He/she can then eavesdrop on a path to capture all or the majority of the packages of a connection. Hence the current use of Dijkstra's algorithm in OSPF leads to path predictability and becomes a security risk. One way to mitigate this risk is to encrypt all network traffic including both user data packages as well as the Link State Advertisement messages. However this approach requires significantly more computing power from the router [9]. In our proposed solution we attempt to make the routing paths less predictable thus making it more difficult for an attacker to eavesdrop on user traffic. For each destination, instead of having only one next-hop entry in the routing table, we propose to have multiple entries thus the data packets may reach the destination on different paths. Past work done by researchers, such as proves that algorithms exist that also find more than one disjoint paths. The disadvantages of these algorithms are that an increased number of control messages are created and they assume no topology changes may occur during the path finding procedure [10].

Some researcher's et al. proposed a path randomization for dynamic routing, but they focus only on Routing Information Protocol (RIP) for wired networks [11].

In this paper, we propose a new routing algorithm to enhance the security of the Internet. Instead of using Dijkstra's algorithm to find only one shortest path between each pair of source-destination nodes, we will find multiple paths between each pair of source-destination nodes. We will then populate the routing table with all the paths. When a data package arrives as a router, instead of always sending the package by the same path, the router will randomly choose one of the paths in the routing table to send the package by. Because the path is randomly selected for each package, it becomes more difficult for an attacker to eavesdrop all packages of a communication session. This layer of added security conceals the package's path and therefore better protects against interception, spoofing and redirecting. Here is how the rest of the paper is organized. In Section 2, we first describe the Dijkstra's Algorithm and its security vulnerability.

2. Proposed Routing Algorithm:

Shortest-path algorithms such as Dijkstra's Algorithm [13] are integral part of the OSPF routing protocol. After a router has established the topology of the network, it uses Dijkstra's Algorithm to compute the best paths between the source-router and all possible destinations. It then populates the IP routing table with the lowest cost path for each destination. Every router has its own IP routing table which dictates where each data package is forwarded to. The algorithm begins with marking all nodes to be unvisited, the initial node cost to be zero and every other node cost to be infinity. First, let the starting node be the current node and then consider the cost to reach all of the current node's neighbours. Then, compare this value to the currently assigned cost to the node and assign the smaller value. Next, mark the current node as visited and choose the unvisited node with the lowest cost as your next current node. The algorithm will continue moving through the network in this way until all nodes have been visited. The running time of the Dijkstra's algorithm is O(|V|2) or O(|E| + |V| log |V|), where |V| is the number of vertices and |E| is the number of edges in the network [14]. This is an efficient and seamless process to find the lowest cost path from the starting node to every other node in a network. The downside is that Dijkstra's Algorithm is a well-known algorithm. Once the topology is known, an attacker can compute the exact path by which any data packages will be sent. This kind of information can facilitate an attacker to intercept, redirect and spoof data packages [15]. Even though we can encrypt all the traffic to increase security, it is not ideal to completely rely on encryption. The network traffic can be better protected if the paths taken by the packets are less predictable.

A. Comparison between Routing Algorithms:

With the Hot Potato Routing algorithm, the path by which a package travels is completely random. The way this algorithm works is when a packet is received by a router, the packages are randomly forwarded to one of the router's neighbours [15]. The router does not take into consideration the ending node, the link costs or path minimization. This way the path by which a package travels is completely random. The positive aspect of this algorithm is that it provides more security against spoofing and sniffing because it is impossible for a hacker to determine the path or to track the data packages. However, this Hot Potato Algorithm is very inefficient as the paths may end up being very long. Consider a data packet received by router A and is destined to A's neighbouring router B. With this algorithm, router A may send the packet on a path through many other routers instead of directly to B. In small networks this might not be a huge deal, but in a very large network this will substantially increase the time it takes for a package to reach its destination.

Although the path may be very difficult for an attacker to track, the lack of efficiency makes this protocol impractical [16]. Cold-potato routing, on the other hand, is more expensive to do, but keeps the traffic under the network administrator's control for longer, allowing operators of well-provisioned networks to offer a higher quality of service to their customers. It can also be preferred when connecting to content providers; if content providers use hot-potato routing, they may escape from paying for the cost of links between cities. Cold-potato routing is prone to bad configuration as well as poor coordination between two networks. In such scenarios, packets can be routed further distances and can allow another autonomous system to manipulate routing in a network for various purposes. Cold-potato routing requires a level of trust between two networks that either side will not attempt to "cheat" the other.

Some content networks favour the use of cold-potato routing in order to deliver content from replicated server farms closer to the end-user. In the next algorithm, we will combine the strengths of the Hot Potato algorithms and the Dijkstra's Algorithm to provide a more secure but also efficient way of forwarding data packets.

B. Dynamic Random Path Selection (DRPS):

As we saw, Dijkstra's algorithm is a good way to ensure the path to the end node is always the shortest one. This is important as the routing process must be very efficient. Therefore, in our approach we also use Dijkstra's algorithm but we run the algorithm multiple times in order to find multiple shortest paths to an end node. Later when a data package arrives at the router, the router forwards the package to one of its neighbouring routers which are on the previously computed paths to the destination. While this approach adds a little more work for the router when populating its routing table, it will boost our network confidentiality and ensure the integrity of the data packages. In the implementation of Dijkstra's algorithm, to send a package between two neighbouring routers, let's say node A to node B, there must be a quantified cost assigned to the link. On the other hand, if there is no link between the routers the cost for the link is set to infinity and the two routers are not change the link cost of all the links used in that path to be infinity.

Basically, we will remove the shortest path from the set of available routes to send data by. We then run Dijkstra's algorithm again to find another path which will be link disjoint from the first one. We will keep repeating this process until we obtain the desired number of disjoint paths. Lastly, the router will save all of the paths found into its routing table, which will ensure we will have access to all paths later when the router needs to route a data package. We may exclude the next-hop on the shortest path to further improve the security as discussed later [17]. At this point all our network paths are computed and we can start forwarding the packages. Each time a data package is received, the router will randomly choose one of the paths which it has computed earlier to send the package by. By creating this randomization process, we expect to lower the chances for an attacker being able to track and find the packages as they travel through the network. In the case when an attacker is able to calculate the shortest path between the source node and the destination node and he/she is also able to gain access to one of the links on the path, the attacker can capture all traffic from the source node to the destination node if the routers are running Dijkstra's Algorithm and hence all packets pass through the same path. On the other hand, if the routers are running either the Hot Potato Routing algorithm or the DRPS algorithm, the amount of packets being captured by the attacker may be significantly reduced. We can calculate the upper bound on the amount of traffic captured by the attacker in the latter cases as follows. For the DRPS algorithm, let n to be the number of next-hop entries in the routing table stored for each destination, then the average amount of traffic may be captured by an attacker is 1/n of the total traffic if the attacker has access to one of the links on the shortest path. The larger n is, the more difficult for an attacker to capture all packets. If the n entries in the routing table exclude the next-hop on the shortest path, then the amount of traffic may be captured by an attacker is zero.

For the Hot Potato Algorithm, each packet travels on a random path before reaching the destination node. The amount of traffic captured by the attacker depends on the nodal degree of the network, as well as on the attacker's hop distance to the source node and the destination node. Let the nodal degree to be d. Also assume the attacker have access to the i-th link on the shortest path from the source node thus 1 i h, or equally the (h - i + 1)-th link to the destination node. When min(i, h - i + 1) = 1 where function min(x, y) returns the lesser value of x and y, the packets from the source node to the destination are equally distributed on d paths, then the average amount of traffic may be captured by an attacker is 1/d of the total traffic. For other values of min(i, h - i + 1), the traffic from the source node to the destination are equally distributed on dmin(i, h - i + 1) paths, thus considered neighbours. This is important for the algorithm to determine whether or not to send a package through that path. Our solution utilizes this same principle of the algorithm [18].

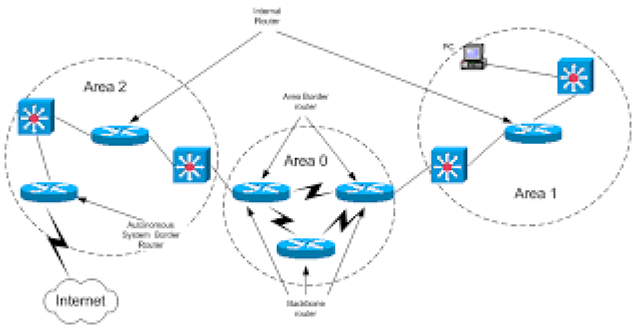


Figure.1. Architecture for Advanced Open Shortest Path First (AOSPF)

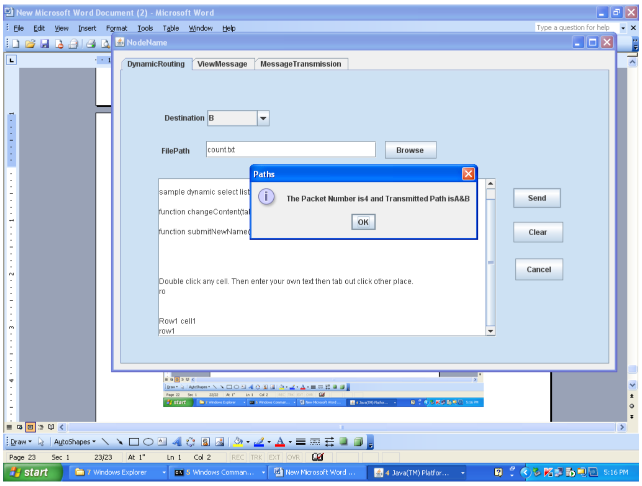
The first step is to run the algorithm like it would normally be run in OSPF. Then OSPF will be increased with advanced clustering algorithm [18]. It classifies working of routers and paths in the network. If a route is failure then automatically the alert will goes to central system. Advanced OSPF describes active shortest paths in the network as well as dead paths in the network. So the When the shortest path is selected and saved, we the average amount of traffic may be captured by an attacker is 1/ d min(i, h - i + 1) of the total traffic.

Lager nodal degree d makes it more difficult for an attacker to capture all packets.With either the Hot Potato Routing Algorithm or the DRPS Algorithm, the paths travelled by the data packets may be longer than that of the paths generated by a shortest path algorithm such as Dijkstra's algorithm. With additional path length, there may be more packets travelling in the network at any given moment which may require more network resource to process these packets.

3. RESULTS AND DISCUSSION:

In this section we conduct computer simulations to determine the effectiveness of the Disjoint Path Routing with Random Selections (DPRRS) algorithm. We have three variations for the DPRRS algorithm: DPRRS-2, DPPRRS-3, and DPRRS-4, with which a router randomly chooses one of two, three, and four disjoint paths respectively from its routing table to the destination node. We compare their performance with those of the Hot Potato Routing and those of the Dijkstra's algorithm. We use LEDA programs to randomly generate network graphs of sizes ranging from 10, 20 and 40 nodes and a nodal degree (i.e., the number of links ending in a node) of 2.8.

As mentioned at the end of Section II, longer routing paths can lead to additional network resource consumption and longer delays experienced by network users. Since the most significant network resource consumptions and delays occur at the routers, we run the algorithms on these networks and compare the average hop-counts between all node-pairs of the networks. A hop-count is the number of routers on a path connecting the source node and the destination node. It equates to path length when all link cost is 1.



Destination B

FilePath count.txt

sample dynamic select list
function changeContent(tal
function submitNewName(

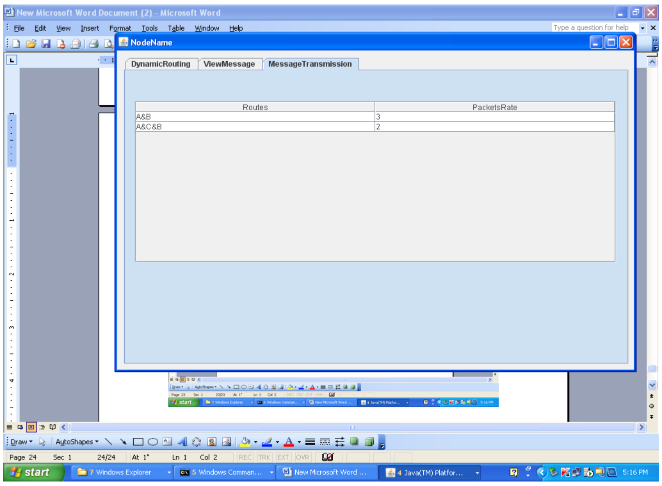
Double click any cell. Then enter your own text then tab out click other place.
ro

Row1 cell1
row1

The Packet Number is4 and Transmitted Path isA&B

Figure.2. Secure information transfer from sender to receiver.

From the above algorithm, Firstly a network is created which consist of different clusters and based on route levels of each node the cluster heads are elected. To forward a data within a distinct source node and destination nodes are selected. To increase system lifetime we have to detect malicious routes which are responsible for secure information throughout the internet [19]. Figure 2 shows transferring of information from source to destination with secure manner. Figure 3 shows total number of routes and nodes participation in the net work. That information taking from sender point to destination point without any disturbance.To detect compromised nodes from WSN, we are using acknowledgement based IDS. When the forwarded data is received at the receiver side, then it sends acknowledgement to the sender node. The ACK is compared with the size of received data; if it is equal then data forwarded-successfully with no loss in packets, otherwise it will detect loss in the packet.



Routes	PacketsRate
A&B	3
A&C&B	2

Figure.3 Total number of dynamic routes in the network.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The data from the simulation is contained in Table 1 and depicted in Fig 1 and Fig 2. As expected, with the Hot Potato Routing algorithm, a router passes an incoming packet to one of its neighbouring routers at random, thus the packet is likely to experience the longest path length and delay before reaching its final destination. In the worst case, a packet may be travelling in circles in the network while not reaching the destination. On the other hand, with Dijkstra's Algorithm, a router always passes an incoming packet to its neighbour who is on the shortest path to the packet's final destination, thus the packet always experience the shortest path and delay. DPRRS algorithms generate paths whose hop counts are slightly higher than that of Dijkstra's Algorithm but significantly lower than that of the Hot Potato Routing algorithm [20]. Out of the three variations of DPRRS algorithms, DPRRS-2 has the hop counts that are closest to that of Dijkstra's Algorithm while DPRRS-4 has the largest difference. This can be explained as follows. When each router has a larger collection of neighbouring routers to forward an incoming packets, there are more variations of possible paths for the packets to reach their destination which cause the paths average hop counts to increase.

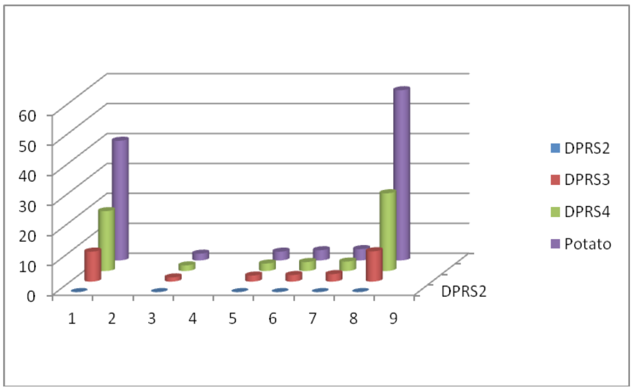


Figure.4 Comparison of dynamic routing algorithms.

Figure 4 shows the comparison between all routing algorithms. But potato method combined with dynamic random path selection, finally it shows optimal routing in wireless networks.The aim of our system is to increase lifetime and security in the network, in the first graph we shows that how we increased lifetime and this graph shows the time required for sending the specific size of data with and without security, as we are providing the security the time should be more as compared to normal sending for security we are using the encryption algorithm for security.

4. CONCLUSION:

In this paper, we proposed a new routing algorithm that enhances network security against eavesdropping attacks. The algorithm's complexity is polynomial and can be easily implemented. Provide security for redun¬dancy management of clustered wireless networks by utilizing multipath routing to answer user queries. In our work, we consider redundancy management of mul¬tipath routes, based on trust and energy values, for intru¬sion detection, and to maximize the system lifetime of a WSN in the presence of unreliable and malicious nodes. We have noted that increasing source redundancy as well as path redundancy will enhance the reliability and se¬curity. However, it also decreases the energy consump¬tion and thus it contributing to the increase of the system lifetime. Computer simulations reveal that the algorithm causes the hop counts hence the network delay to increase only by a limited amount. For future study, we will investigate the optimal degree of path randomness for a given protection objective.

5. REFERENCES:

[1] W. Guo, W. Zhang, A survey on intelligent routing protocols in wireless sensor networks, Journal of Network and Computer Applications, 38 (2014) 185-201.

[2] J. Yang, M. Xu, W. Zhao, B. Xu, A multipath routing protocol based on clustering and ant colony optimization for wireless sensor networks, Sensors, 10 (2010) 4521-4540.

[3] M. Burmester and T.V. Le, "Secure Multipath Communication in Mobile Ad Hoc Networks," Proc. Int'l Conf. Information Technology: Coding and Computing, pp. 405-409, 2004.

[4] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," IEEE Comm. Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002AI Magazine, vol. 18, no. 4, pp. 97–136, 1997.

[5] W. Lou and Y. Kwon, "H-Spread: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks," IEEE Trans. Vehicular Technology, vol. 55, no. 4, pp. 1320- 1330, July 2006.

[6] P. Papadimitratos and Z.J. Haas, “Secure Routing for Mobile Ad Hoc Networks,” Proc. SCS Comm. Networks and Distributed Systems Modeling and Simulation Conf. (CNDS), 2002.

[7] Rao, Gudikandhula Narasimha, and P. Jagdeeswar Rao. “A Clustering Analysis for Heart Failure Alert System Using RFID and GPS.” ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol I. Springer International Publishing, 2014.

[8] H. Yang, F. Ye, Y. Yuan, S. Lu, and W.Arbaugh, Toward Resilient Security in Wireless Sensor Networks,” Proc. ACM MobiHoc, 2005.

[9] G. Narasimha Rao, R. Ramesh, D. Rajesh, D. Chandra sekhar.”An Automated Advanced Clustering Algorithm For Text Classification”. In International Journal of Computer Science and Technology, vol 3,issue 2-4, June, 2012, eISSN : 0976 - 8491,pISSN : 2229 – 4333.

[10] K. D. Kang, K. Liu, and N. Abu-Ghazaleh, “Securing geographic routing in wireless sensor networks,” in Proc. 2006.

[11] W. Lou and Y. Kwon, “H-SPREAD: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks,” IEEE Trans. Veh. Technol., vol. 55, no. 4, pp. 1320–1330, 2006.

[12] N. Kimura and S. Latifi, “A survey on data compression in wireless sensor networks,” in Proc. Int. Conf. Inf. Technol., Coding Comput., 2005, vol. 2, pp. 8–[13] F. Sebastiani, “Machine learning in automated text categorization,” ACM Comput. Surveys, vol. 34, no. 1, pp. 1–47, 2002.

[14] J. H. Cho, I. R. Chen, and P. G. Feng, “Effect of intrusion detection on reliability of mission-oriented mobile group systems in mobile ad hoc networks,” IEEE Trans. Reliab., vol. 59, no. 1, pp. 231–241, 2010.

[15] Y. Zhou, Y. Fang, et.al., “Securing wireless sensor networks: a survey,” IEEE Commun. Surveys & Tutorials, vol. 10, no. 3, pp. 6–28, 2008.

[16] I. Guyon and A. Elisseeff, “An introduction to variable and feature selection,” J. Mach. Learn. Res., vol. 3, pp. 1157–1182, 2003.

[17] I. Guyon, C. Aliferis, and A. Elisseeff, “Causal feature selection,” in Computational Methods of Feature Selection Data Mining and Knowledge Discovery Series, Boca Raton, FL, USA: CRC, 2007 pp. 63–85.

[18] A. Nanopoulos, R. Alcock, and Y. Manolopoulos, “Feature-based classification of time-series data,” in Information Processing and Technology, Commack, NY, USA: Nova, 2001 pp. 49–61.

[19] B. Balaji Bhanu , Dr. P. Srinivasulu, Gudikandhula N Rao, ”Secure Group Key Communication in Sensor Networks” In International Journal of Advanced Computer Engineering and Architecture, Vol. 2 No. 1 (January- June,2012) ISSN: 2248-9452.

[20] Thomas Stimpson et al., “Assessment of Security and Vulnerability of Home Wireless Networks”, Proc. of 9th Int. Conf. fuzzy systems & knowledge discovery, Chongqing, pp. 2133-2137, May, 2012.