International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 6, August - 2012

An Efficient Routing Protocol with Dynamic Security Considerations

Dr. K. Rama Krishnaiah, Mrs. Kompalli Udaya

Abstract—Security has become one of the major issues for data communication over wired and wireless networks. 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 compatible with popular routing protocols, such as the Routing Information Protocol in wired networks and Destination-Sequenced Distance Vector protocol in wireless networks, without introducing extra control messages. Increasing power consumption and packet storming within ad-hoc network is becoming a core issue for these low power mobile devices. In this work, we propose an improvement on DSDV protocol to allow sleep mode to take part in communication of the ad-hoc network. This work focuses on energy conservation as well as reducing packet storming within the routing protocol of the ad-hoc network. A wireless network interface in sleep mode consumes less power than idle mode.

I INTRODUCTION

Existing work on security-enhanced data transmission includes the designs of cryptography algorithms and system infrastructures and security-enhanced routing methods. Their common objectives are often to defeat various threats over the Internet, including eavesdropping, spoofing, session hijacking, etc. Among many well-known designs for cryptography based systems, the IP Security (IPSec) and the Secure Socket Layer (SSL) are popularly supported and implemented in many systems and platforms. Although IPSec and SSL do greatly improve the security level for data transmission, they unavoidably introduce substantial overheads, especially on gateway/host performance and effective network bandwidth. For example, the data transmission overhead is 5 cycles/byte over an Intel Pentium II with the Linux IP stack alone, and the overhead increases to 58 cycles/byte when Advanced Encryption Standard (AES) is adopted for encryption/decryption for IPSec.

Another alternative for security-enhanced data transmissions 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.

Later, a dynamic routing algorithm was proposed 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 in wired networks and Destination-Sequenced Distance Vector protocol in wireless networks, without introducing extra control messages. Proposed a secure routing protocol to improve the security of end-to-end data transmission based on multiple path deliveries. But there are several problems with DSDV protocol:

- It is silent about energy conservation at nodes that is every node in the network should be active all the time in the communication process even if some of them are not currently taking part in the data forwarding process. So that unnecessarily energy is wasted at the nodes.

- Another problem is packet storming that is even if there is no data communication taking place still control packets are transmitted among nodes consuming much of the bandwidth.
- It only considers hop count as metric but is not considering efficiency (processing speed) of nodes.
- It is also not considering the status (free/busy) of internal nodes.
- It is also silent about the convergence.

In this paper to address the above problems, we propose an improvement on DSDV protocol to allow sleep mode to take part in communication of the ad-hoc network to reduce power consumption. This work focuses on an approach for energy conservation as well as reducing packet storming within the routing protocol of the ad-hoc network. A wireless network interface in sleep mode consumes less power than idle mode. Sleep mode has very low power consumption. The network interface at a node in sleep mode can neither transmit nor receive packet. It must be wake up to idle mode first by explicit information from the node.

II REALTED WORK

A) 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.

B) 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.

C) Zone Routing Protocol

The Zone Routing Protocol (ZRP) 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.

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.

III. PROPOSED SYSTEM

We will propose a dynamic routing algorithm 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 in wired networks and Improvised Destination-Sequenced Distance Vector protocol in wireless networks, without introducing extra control messages.

A) Routing Information Protocol (RIP)

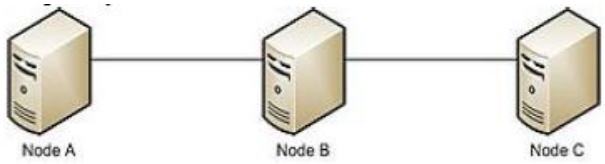
The Routing Information Protocol (RIP) is a distance-vector routing protocol, which employs the hop count as a routing metric. The hold down time is 180 seconds. This protocol prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 is considered an infinite distance and used to deprecate inaccessible, inoperable, or otherwise undesirable routes in the selection process.

RIP implements the split horizon, route positioning and hold-down mechanisms to prevent incorrect routing information from being propagated. These are some of the stability features of RIP. It is also possible to use the so called RMTI (Routing Information Protocol with Metric-based Topology Investigation) algorithm to cope with the count-to-infinity problem. With its help, it is possible to detect every possible loop with a very small computation effort.

B) Destination-Sequenced Distance-Vector routing

Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for adhoc mobile networks based on the Bellman-Ford algorithm. The main aim 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 or else an odd number is used. The number is generated by the destination, and the emitter has to send out the next update with this number. Routing information is distributed among the nodes by sending full dumps infrequently and smaller updates more frequently which are incremental.

The procedure in selection of router is as follows. 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, then the route with the better metric is used. The entries that have not been updated for a while are called stale entries. Such entries and the routes using those nodes as next hops are deleted.



For example the routing table of Node A in this network is

Destination	Next Hop	Number of Hops	Sequence Number
A	A	0	A46
B	B	1	B36
C	B	2	C28

Naturally the table contains description of all possible paths reachable by node A, along with the next hop, number of hops and sequence number.

C) Improvised Destination-Sequenced Distance-Vector routing

Every node in network can interleave between sleep mode and idle mode. Sleeping condition of a node is the condition that every node in the network knows that the node is in sleep mode but that node will interleave between sleep mode and idle mode, during that sleeping condition without revealing to the network. A node can go to sleep mode when it will only receive control packet for some fixed amount of time. The time may not same for each node in the network that is every node will take a random amount of time.

When a node ready to go to sleep node it will transmit a control message indicating its address. When all other nodes receive that message will update their routing table by setting a flag for that node. After a node going to sleep mode it will periodically wake up to idle mode but it will not revel this information to the network.

When a node is in sleeping condition and receives a sleep mode message of another node it will just update the table for that node but will not wake up.

When a node gets a request to wake up message (RW) then it will reveal that it is wake up by sending a wake up message containing its routing table information to its neighbors. It will remain in wake up state during data packet forwarding or receiving.

Sending and receiving

When a node is in sleeping condition and wants to transmit data to another node which is in wake up state then first it will wake up and broadcast wake up message along with current routing table information. When its neighbors get wake up message they will also wake up and also update its table and then according to current table information sender will send data packet.

When a node wants to send data to another node that is in sleeping condition then it will first broadcast RW message by Flooding. When any sleeping node receive that RW message will wake up and communicate as usually.

IV ROUTING WITH SECURITY CONSIDERATIONS

For security purpose, for delivering a data packet we use randomization process and maintain routing table based on bell-men ford algorithm.

A) 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. In this process, the previous nexthop hs for the source node s is identified in the first step of the process. Then, the process randomly picks up a neighbouring node in excluding hs as the nexthop for the current packet transmission. The exclusion of hs 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.

B) 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.

Bellman-Ford algorithm computes single source shortest paths in a weighted digraph. For graphs with only non-negative edge weights, the faster Dijkstra's algorithm also gives solution to the

problem. Thus, Bellman–Ford is used for graphs with negative edge weights. Bellman–Ford's basic structure is very similar to Dijkstra's algorithm, but instead of greedily selecting the minimum-weight node not yet processed to relax, it simply relaxes all the edges, and does this $|V| - 1$ times, where $|V|$ is the number of vertices in the graph. The repetitions allow minimum distances to accurately propagate throughout the graph, since, in the absence of negative cycles, the shortest path can only visit each node at most once. Unlike the greedy approach, which depends on some specific structural assumptions derived from positive weights, this straightforward approach extends to the general case.

V CONCLUSION

Various security-enhanced measures have been proposed to improve the security of data transmission over public networks. In this paper, we propose a secure-enhanced dynamic routing algorithm 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 in wired networks and Destination-Sequenced Distance Vector protocol in wireless networks, without introducing extra control messages. In this paper, we propose an improvement on DSDV protocol to allow sleep mode to take part in communication of the ad-hoc network to reduce power consumption. This work focuses on an approach for energy conservation as well as reducing packet storming within the routing protocol of the ad-hoc network. A wireless network interface in sleep mode consumes less power than idle mode. Sleep mode has very low power consumption.

VI REFERENCES

[1] C. Siva Ram Murthy and B. S Manoj, "AdHoc Wireless Networks, Architecture and Protocols", Prentice Hall PTR, 2004.
[2] Dynamic routing with security Considerations IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL.20, NO.1, JANUARY2009 Chin fu kuo , Member, IEEE , Ai-Chun Pang , Member , IEEE .
[3] I.Gojmerac, T.Ziegler, F. Ricciato and P. Reichl "Adaptive Multipath Routing for Dynamic Traffic Engineering" Proc. IEEEGlobal TeleCommunications Conference.
[4] C. Kaufman, R. Perlman, and M. Speciner, Network Security—PRIVATE Communication in a PUBLIC World, second ed. Prentice Hall PTR, 2002.
[5] DSDV (Highly Dynamic Destination-Sequenced Distance Vector routing protocol) - C. E. PERKINS, P. BHAGWAT Highly Dynamic Destination- Sequenced Distance Vector (DSDV) for Mobile Computers Proc. of the SIGCOMM 1994 Conference on Communications Architectures, Protocols and Applications, Aug 1994, pp 234-244.
[6] L. Feeney and M. Nilsson. Investigating the Energy Consumption of a Wireless Network Interface in an Ad Hoc Networking Environment. In Proceedings of INFOCOM 2001, volume 3, pages 1548–1557, Anchorage, Alaska, Apr. 2001.
[7] S. PalChaudhuri. Power Mode Scheduling for Ad Hoc Network Routing. Masters Thesis, Computer Science, Rice University, May 2002.
[8] 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.

Authors:

Dr. K. Rama Krishnaiah is a highly qualified person holding **M.Tech** and **Ph.D** degree in **CSE,** an efficient and eminent academician. He is an outstanding administrator, a prolific researcher, who has published 21 research papers in various international journals and a forward looking educationist. He worked in prestigious **K L University** for 13 years and he contributed his service for NBA accreditation in May 2004, Aug 2007 with 'record rating', ISO 9001:2000 in 2004, Autonomous status in 2006, NAAC accreditation of UGC in 2008 and University status in 2009.

Mrs. Kompalli Udaya Sri, received her M.B.A., Degree in Finance from Dr. B.R. Ambedkar Open University, Hyderabad, in the year 2004 and

M.Sc Degree in Information Technology from Acharya Nagarjuna University, in the year 2010 and presently she is pursuing **M.Tech.** in Computer Science & Engineering from the year 2010 and about to complete her M.Tech in the year 2012 from Nova College of Engineering and Technology for Women, Jupudi, affiliated to Jawaharlal Nehru Technological University, Kakinada.