SEAP: Secure Efficient Path Vector Routing Mobile Wireless Ad Hoc Networks

Dr.K.Ravikumar[1]
Dept of Computer Science,
UGC – NET Coordinator,
Asst. Professor, Tamil University,
Thanjavur.India

R.Suganya[2]
Dept of Computer Science,
Asst.Prof & Research Scholar,
T.U.K Arts &Science College,
Thanjavur.India

T.Sakthialamelu[3]
Dept of Computer Science,
Asst.Prof,
T.U.K Arts &Science College,
Thanjavur.India

Abstract

An ad hoc network is a collection of wireless nodes, communicating among themselves and road-side infrastructure such as base station. Vehicular ad hoc networks routing protocols have been based on path vector approaches. In this paper, we design and evaluate the secure efficient ad hoc path vector routing protocol (SEAP), a secure ad hoc routing protocol based on the design of the direct path distance vector routing protocol. In order to support we use with nodes of limited CPU processing capability, and to redirect the DOS attacks attempt to cause other nodes to excess network bandwidth or processing. We use efficient one way hash functions. SEAP performs well directly deliver of packet from routing table in any other node, even in spite of any active attackers or multi – hop nodes in the network.

Keywords: *Mobile ad hoc network, ad hoc network routing, secure routing, SEAP, one way hash function, path distance vector.*

1. Introduction

In a mobile wireless ad hoc network, computers in the network co operate to forward packets for each other, due to the limited wireless transmission range of each individual node. The network route from some sender node to a destination node may require a number of intermediate nodes to forward packets to create a "multi hop "path from this sender to the destination.

In this paper, we focus on securing ad hoc networks routing using periodic protocols, and in particular using path vector routing protocols. A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route[1][2].

Each router has a prior knowledge only of network attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, router gains the knowledge of the topology of the network.

We present the design and evaluation of a new secure ad hoc network routing protocol using path vector. Our protocol, which we call the Secure Efficient path vector routing protocol (SEAP). Path selection involves applying a routing metric to multiple routes in order to select (or predict) the best route. Cisco routers, for example, attribute a value known as the administrative distance to each route, where smaller administrative distances indicate routes learned from a supposedly more reliable protocol [3].

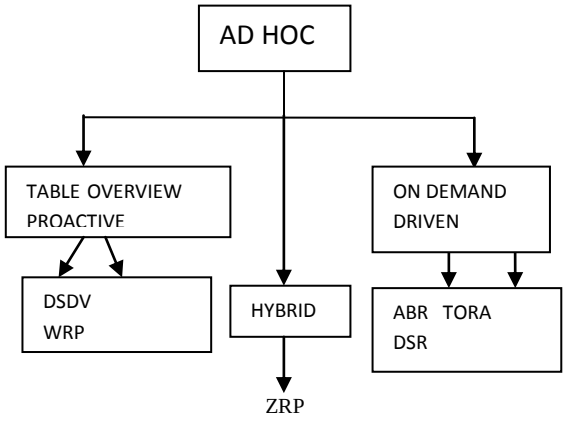

Fig 1: Ad Hoc Mobile Routing

We base the design of SEAP in part on the direct – path distance vector (DPDV) [34] which was designed for trusted environments. In order to support we use of SEAP with nodes of limited CPU processing capability, and to guard against Denial – of-service attacks in which an attacker attempt to

cause other nodes to consume excess network bandwidth or processing time, we use efficient one-way hash functions and use asymmetric cryptographic operations in the protocol.

In section 3 of this paper multipath routing is the routing technique of using multiple alternative paths through a network, which can yield a variety of benefits such as fault tolerance, increased bandwidth, or improved security. The multiple paths computed might be overlapped, edge-disjointed or node- disjointed with each other [5]. Extensive research has been done on multipath routing techniques. Distance vector routing and link state routing are both intra - domain routing protocols. They are used inside an autonomous system, but not between autonomous systems. Both of these routing protocols become intractable in large networks and cannot be used in inter domain routing. Distance vector routing is subject to instability if there are more than a few hops in the domain [6][7].

2. Path vector routing and DPDV

Path vector routing protocol finds best path between nodes in the networks through a disputed implementation of the Jacobi symbol algorithm [8][9]. As noted in section 1 path vector protocols are easy to implement and are efficient in terms of memory and CPU processing capacity required at each node.

When one network goes down , any nodes that used it as their next hop discard the entry, and create new routing – table information[8].These nodes convey the updated routing information to all adjacent nodes, which in turn repeat the process. Eventually all the nodes in the network receive the updates, and discover new paths to all the destinations they can still “reach”. E.g. RIPV1, RIPV2 [9]. (Concurrent multipath Routing) is often taken to mean simultaneous management and utilization of multiple paths for the transmission of streams of data emanating from an application or multiple applications.

This provides better utilization of available bandwidth by creating multiple active transmission queues. It also provides a measure of fault tolerance in that, should a path fail, only the traffic assigned to the path is affected, the other paths continuing to serve their stream flows; there is also , ideally, an alternative path immediately available upon which to continue or restart the interrupted stream.

The stream continues uninterrupted, transparently to the application. This method provides significant performance benefits over the former.

- By continually offering packets to all paths, the paths are more fully utilized.
- No matter how many nodes (and thus paths) fail, so long as at least one path constituting the virtual path is still available, all sessions remain connected. This means that no streams need to be restarted from the beginning and no reconnection penalty is incurred.
- The primary improvement to ad hoc network made in DPDV order standard path vector routing is addition of a sequence number in each routing table entry. The use of this sequence number prevents routing loops caused by updates being applied out of order. Since the routing information may spread along many different paths through the networks [9].
- Each node maintains an even sequence number that it includes in each routing update that it sends, and each entry in a nodes routing table is tagged with the most recent sequence number it knows for that destination. When a node detects a broken link to a neighbor, the node creates a new routing update for that neighbor as a destination.

Path vector routing is discussed in RFC [10][11]; the path vector routing algorithm is somewhat similar to the distance vector algorithm in the sense that each border router advertises the destinations it can reach to its neighboring router. However, instead of advertising networks in terms of a destination and the distance to that destination, networks are advertised as destination addresses and path descriptions to reach those destinations.

A route is defined as a pairing between a destination and the attributes of the path to that destination, thus the name, path vector routing, where the routers receive a vector

that contains path to a set of destinations. The paths, expressed in terms of the domains (or confederations) traversed so far, is carried in a special path attribute that record the sequence of routing domains through which the reach ability information has passed.

3. Assumption

In this paper, we use "MAC" to refer to the network medium Access control at the link layer, and not a message authentication code used for authentication. Network physical layer and MAC layer attacks are beyond the scope of this paper [11][12]. Use of spread spectrum has been studied for securing the physical layer against jamming [13].MAC protocols do not employ some form of carrier sense, such as ALOHA and slotted ALOHA [11], are less vulnerable to denial - of – service attacks, although they generally use the channel less efficient.

We assume that nodes in the ad hoc networks may be resource constrained. Thus, in securing our path vector ad ho networks routing protocol SEAP. We use efficient one-way hash chains [13] and merle hash tree [14] rather than relying on expensive asymmetric cryptographic operations.

3.1 One – way hash chains:

A one – way hash chain is built on a one- way hash function. Like a normal hash function, a one –way hash function, H, maps an input of any length to affixed length bit string. Thus, H :{ 0, 1}*→ {0, 1}$^{\rho,}$ where ρ is the length in bit of the output of the hash function.

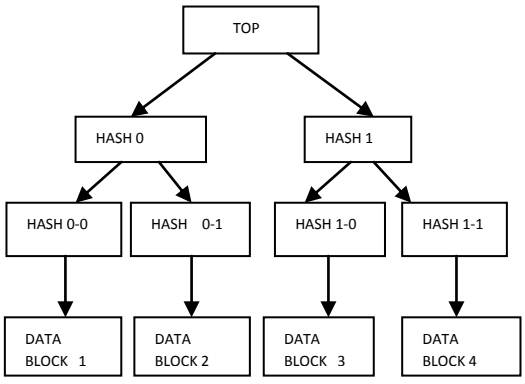

Fig 2: One-Way Hash Functions

The function H should be simple to compute yet must be computationally infeasible in general to invert. A more formal definition of one –way hash function is provided by goldwasser and has been proposed, including MD5 [14] and SHA-1 [12].

To create a one –way hash chain, anode chooses a random initial value xϵ{0,1}$^{\rho}$ and computes the list of values. h_0, h_1, h_2 . . . , h_n where h_n = x, and h_1=H(h_{i-1}) for 0< I <=n, for some n. the node at initializations generates the elements of its hash chain as shown above, from "left to right" and then over time uses certain elements of the chain to secure its routing updates; in using these values , the node progresses from "right to left" within the generated chain.

Given an existing authenticated element of one – way hash chain, it is possible to verify elements later in the sequence of use within the chain (further to the left, or in order to decreasing subscript). For example, given an authenticate h_{i-3} by computing H (H (H (h_{i-3}))) and verifying that the resulting value equals h_i.

3.2. Tree– authenticated values:

Merkle tree is a tree in which every non- leaf node is labeled with the hash of the labels of its children nodes. Hash tree are useful because they allow efficient and secure verification of the contents of larger data structure. Hash tree are a generalization of hash lists and hash chains. To demonstrate that a leaf node is a part of a given hash tree requires an amount of data proportional to the log of the number of the nodes of the tree. (This contrasts with hash lists, where the amount is proportional to the number of nodes). The concept is named after Ralph Merklle.

4. Attacks:

Kumar [12] and smith et al[14] discuss attacks against distance vector routing protocols. In addition, in prior work we presented some attacks against ad hoc network routing protocols against [11]. In this section,

we summarize relevant attacks.An attacker can attempt to reduce the amount of routing information available to other nodes, by failing to advertise certain routes or by destroying or discarding routing packets. A node failing to advertise a route indicates its unwillingness to forward packets for those destinations. We do not attempt to defend against this attack, since the attacker could also otherwise drop data packets sent to those destinations. A node can drop routing packets it receives, in which case it becomes ignorant of links available to it and fail to pass potentially improved knowledge to its neighbors.

5. Securing path vector routing

5.1. Basic design of SEAD

We base the design of our secure routing protocol SEAP on the DPDV- see of the ad hoc network routing protocol, as described in section 2. In particular, to avoid the long – lived routing loops in SEAP, we use destination sequence number as in DPDV, we also use the best path of routing update messages in SEAP.We differ from DPDV in that an average message to send the path vector. To reduce the number of redundant triggered updates, each node in DPDV, for each destination to identify the best path of routing protocol.

In addition, unlike DPDV, when a node detects that its next – loop link to some destination is broken, the node does not increment the sequence number for that destination in its routing table when it sets the metric in that entry to infinity.

5.2 metrics and sequence number authenticators:

In addition to the difference between our SEAP protocol and DPDV described in section 5.1, the lower bound on each metric in a best route in SEAP is secured through authentication; in addition, the receiver of SEAP routing information also authenticates the sender. One possible approach that could be used for authenticating routing updates in a path vector routing protocol is for each node to sign each of its routing updates using asymmetric cryptography.

First, an attacker could send a large number of arbitrary forged routing updates to some victim node, such that the victim is forced to spend all of its CPU resources attempting to verify this stream of updates, creating an effective Denial – of – service attacks; this attacks ad hoc network nodes tend to have less powerful CPU s then workstation in wired networks.

Second, an attacker who has compromised a node can send updating claiming that any other node is neighbor, causing other nodes packets are delivered from routing table. Finally, even with no attacker present the larger signatures and longer signature generation and verification times of asymmetric cryptography would resource that could otherwise be used for running useful applications and doing useful communication; this problem is more severe in an ad hoc network than in a traditional network due to the limited resources of nodes and links in an ad hoc network, such as available bandwidth, CPU capacity and battery power.

As noted in section 3, we assumed that a bottom of the figure, we use the packets to the sender sends in each time interval, for each packets, the sender uses the key that computes to the time interval to compute the MAC of the packet. For example, for packets pj+3, the sender computes a MAC of the data using key k_{i+1}.Assuming a key disclosure delay of two time intervals (d=2), packets p j+3 would also carry key k_{i-1}.

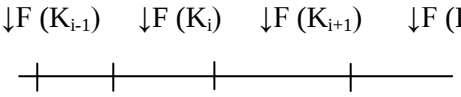

Fig 3: MAC Layer Interval

In particular, these MAC layer approaches authenticate the transmitting source of a packet and ensure that this transmitting source is within some path of the receiver.

5.3. Neighbor authentication:

The source of each routing update message in SEAP must also be authenticated, since otherwise, an attacker may be able to create routing table. An efficient broadcast

authentication mechanism, such as TESLA [9].ZRP [14],TIK[15],can be used to authenticate the neighbor. The drawbacks of these approaches are that they require synchronized clock, and that they incur either an authentication delay or a relatively high communication overhead.

6. Evaluation

6.1. Security analysis

Securing a path vector protocol seems fundamentally harder than security link state. Since path vector protocols compare the routing table information into a hop count value and a next hop, it is challenging to verify the correctness of the hop count value. If each node corresponds to a single hash tree chain value (r=1), the attacker is forced to advertise metric at best m+1.

6.2. Simulation evaluation methodology:

To evaluate the performance impact of their security approach in SEAP without attackers, we modify the DPDV-SQ implementation in our extension to java / jdk 1.3[5]. Specifically, we increased the size of each routing table update to represent the authentication hash value in each table.

We simulated limited CPU processing capability, and to redirect and DOS attacks attempt to cause other nodes to ensure network bandwidth or processing, we use efficient one way hash functions.

We evaluate SEAP by comparing it to DPDV – SQ, as described in section 2, we measure performance along four metrics.

- Packet delivery ratio, the total over all nodes of the number of application – level packets received, divided by the total number of application – level packet originated.
- Byte overhead: the overall hops of the number of head bytes transmitted.
- Packet overhead: the overall hops of the number of the packet transmitted.
- Medium latency: the median packet delivered latency. Where latency is calculated as packet to the routing table and that packet first being received at the destination.

6.2Experimental setup

We implemented the TESLA protocol on top of the Open SSL library [ ]. It's written in Java and consists of about 100 lines of code.

We used laptops and one PDA, a laptop with a P3 – 1. 2GHz, CPU and 512 MB memory, 348 MB memory.

6.3 simulation results:

The results of our performance of SEAP are shown in fig.3 as function of pause time in the routing table model. Each figure represents the average over randomly generated runs at each pause time, and the error bar shows the 93% confidence intervals; the runs used for SEAP and those for DPDV – SQ were identical.

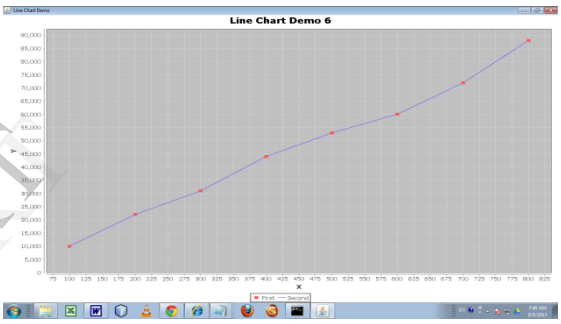

Fig 4: Without Updating Routing Table SEAP & DPDV-SQ

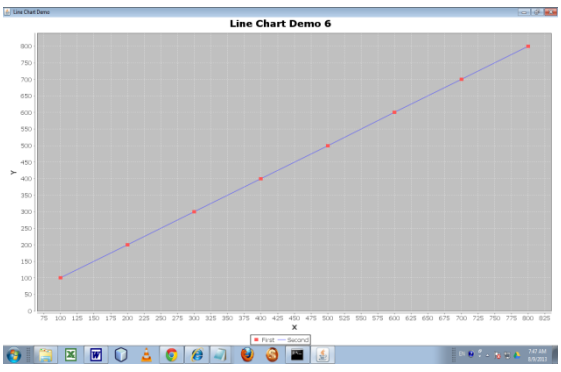

Fig 5: Updating Routing Table SEAP & DPDV-SQ

The product delivery ratio for SEAP and DPDV – SQ are shown in Fig 4 & 5;
X-axis to represents Message Travel Time
Y-axis represents Packet Delivery Ratio .

Source	Base Station	Message Travel Time	Destination
X	A,B,C(3)	3 Min	Y
Y	A,B(2)	3 Min	Y

Table1: SEAD with DSDV

Source	Base Station	Message Travel Time	Destination
X	A,B,C(3)	2 Min	Y
Y	A,B(2)	2 Min	Y

Table 2: SEAP with DPDV

Conclusion:

In this paper, we have presented the design and evaluation of SEAP, a new secure ad hoc network routing protocol using path vector routing many previous routing protocols for ad hoc networks have been based on path vector approaches (e.g [5,12,13,14,15]) but they have generally assumed a trusted environment. Instead, in designing SEAP, we carefully fit inexpensive cryptographic primitives to each part of the protocol functionality to create an efficient, practical protocol that is robust against uncoordinated attackers creating incorrect path routing state in any other node, even in spite of active attackers or compromised nodes in the network.

In future work, we plan to also consider mechanism to detect and expose nodes that advertise routes but do not forward and backward packets, and top merge this work with our other work in security on – demand routing protocols to create a secure protocol based on ZRP [12]. We are also considering the possibility of extending DPDV to behave like a shortest path – vector routing protocol, allowing the source address of each advertisement to be more readily authenticated.

Acknowledgements:

We would also like to thanks the anonymous reviewers, whose comments and suggestion stimulated new thoughts helped to improve the paper.

References:

1.N. Abramson, the ALOHA system – another alternative for computer communications in: Proceedings of the fail 1970 AFIPS Computer Conference, November 1970, pp 281-285.

2.F.Baker, R. Atkinson, RIP – 2 MD5 Authentications, RFC 2082, January 1997.

3.S. Basagni, K. Herrin, E. Rosti, D. Bruschi, Secure pebblenets, in ACM International Symposium on mobile ad hoc networking and computing (MobileHoc 2001), long Beach, CA, October 2001, pp. 156 – 163.

4.Lou, w.& Wu, J. (2007). Toward Broadcast reliabity in Mobile Ad hoc Networks with Double CoveragIEEE Transaction on mobile computing, 6(2), pp. 148 – 163.

5..Perkins, C. E. , & Belding Royer, E. M , (1999). Ad hoc on demand vector routing(AODV) routing,Jdk 1.3/Bin. IETF RFC 3561.

6.B. Kumar, Integration of security in network routing protocols, SIGSAC Review 11(2) (1993) 18 – 25.

7.L. Lamport, password authentication with insecure communications, Communications of the ACM 24 (11) (1981) 770 – 772.

8.G.S. Malkin, RIP version 2 protocol applicability statements, RFC 1722, November 1994.

9B. Bellur, R.G. Ogier, A reliable, dfficient topology, broadcast prototcol & TESLA for dynamic networks, in. proceedings of the 18th annual joint Conference of the IEEE Computer and Communication societies (INFOCOM '99), March 1999, pp, 178 – 186.

10.R. V. Boppana, S. Konduru, an adaptive distance vector routing algorithm for mobile, ad hoc networks, in proceedings of the Twentieth annual joint conference of the IEEE Computer Communication Societies (INFOCOM 2001), 2001, pp. 1753 – 1762.

11. J. Broch, D.A. Maltz, D.B> Johnson, Y. C Hu, J.G. Jetcheva, A Performance comparison of multi – hop wireless ad hoc network routing protocols, in proceedings of the fourth annual ACM/IEEE international conference on mobile computing and networking (MobiCom '98), October 1998, pp. 85 - 97.

12.Kumar & smith an efficient message authentication scheme for link state routing in 13th annual Computer Security Application Conference.

13.M.S.Corson and A. Ephermides, A. Simulated performance study of some distributed routing algorithms for mobile radio networks proc. Johns Hopkins conf., Baltimore, MD, 1983

14.A. Ephermides, J. Wieselthier and D. Baker, A. design concept for reliable mobile radio networks with international journal of wireless & Mobile Networks & ZRP(IJWMN) Vol . 3, No.4, August 2011 frequency hopping signaling Proc IEEE (January 1987).

15.P. Johnsson, T. Larsson, N. Hedman, B. Mielezarek, M. Degermark, Scenarion based performance analysis of routing protocol for mobile ad hoc networks, in preceedings of the 5th annual ACM/IEEE international conference on mobile computing and networking,TIK (MobiCom'99), August 1999, pp. 195 – 206.

Biographics and Photographs

Dr.K.Ravikumar working in Tamil university Thanjavur. He is Presented paper in 50 International and National Conferences and Journals. He is Completed UGC Research Project. He is written 16 DDE Books in Tamil University Thanjavur. He is 12 years Teaching and Research Experience. He is having UGC-NET Coaching Co-coordinator for UGC XI Plan. He is a co-coordinator for DDE courses, Tamil University Thanjavur. His Research Areas is Network Security, Cryptography, Mobile Computing, and Cloud Computing.

Mrs. R. Suganya, working in T.U.K.Arts College, Karanthai, Thanjavur. She is presented paper in 3 International and National Conference and Journals. She is 8 years teaching experience. Her Research area is Network Security, Cryptography and Mobile computing.