ISSN No. 0976-5697

Volume 4, No. 5, May 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Secure DSDV Protocol for Manets

M.Kalavathi
M.Tech(CSE)
School of IT, JNTUH
Hyderabad, India
mkalareddy@gmail.com

K. Suresh Babu
Assistant Professor in CSE
School of IT, JNTUH
Hyderabad, India
kare_suresh@yahoo.co.in

Abstract: This paper presents a secure destination-sequenced distance-vector routing protocol (SDSDV) for ad hoc mobile wireless networks. The proposed protocol is based on the regular DSDV protocol. Within SDSDV, each node maintains two one-way hash chains about each node in the network. Two additional fields, which we call AL (alteration) field and AC (accumulation) field, are added to each entry of the update packets to carry the hash values. With proper use of the elements of the hash chains, the sequence number and the metric values on a route can be protected from being arbitrarily tampered. In comparison with the secure efficient distance vector (SEAD) protocol previously proposed in the literature provides only lower bound protection on the metrics, SDSDV can provide complete protection..

Keywords*: Ad hoc network; routing security; Destination sequenced distance-vector (DSDV); hash chain.*

I INTRODUCTION

A Mobile Adhoc Network is a group of wireless mobile computers in which nodes cooperate by forwarding packets for each other to allow them to communicate beyond direct wireless transmission range. Application such as military exercises, disaster relief, and mine site operation may benefit from adhoc networking, but secure and reliable communication is a necessary prerequisite for such applications. MANETS are more vulnerable to attacks than wired networks due to open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and lack of clear line of defense. Security is a process that is as secure as its weakest link. So, in order to make MANETs secure, all its weak points are to be identified and solutions to make all those weak points safe, are to be considered. So Security issues in MANETs will remain a potential research area in near future.

In recent years, there has been some approaches proposed to secure routing protocols for ad hoc networks, a secure efficient ad hoc distance vector routing protocol (SEAD) based on the insecure DSDV protocol is presented. SEAD uses a one-way hash chain to authenticate the sequence number and metric values on a route. However, we observe that security in SEAD may be further enhanced. Thus, in this work, we also deal with the security issue regarding DSDV protocol. We call our secure version of DSDV secure DSDV (SDSDV).

The rest of this paper is organized as follows. In Section II introduction about MANETS, Section III an overview to DSDV and SEAD protocols, Section IV describes the SDSDV protocol and Section V concluding remarks.

II MOBILE ADHOC NETWORKS

Mobile Adhoc Network (MANET) is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. These networks are fully distributed, and can work at any place without the help of any infrastructure. This property makes these networks highly flexible and robost.

Characteristics

- Communication via wireless means.
- Nodes can perform the roles of both hosts and routers.
- No centralized controller and infrastructure.
- Intrinsic mutual trust.
- Dynamic network topology.
- Frequent routing updates

Advantages

- They provide access to information and services regardless of geographic position.
- These networks can be set up at any place and time.

Applications

- Military or police exercises.
- Disaster relief operations.
- Mine cite operations.
- Urgent Business meetings.

A Classification of Routing Protocols

The knowledge of routing protocols of MANETs is important to understand the security problems in MANETs. The routing protocols used in MANETs are different from routing protocols of traditional wired world. Some of the reasons are listed below:

- Frequent Route updates.
- Mobility.
- Limited transmission range

Periodic routing protocols:

Periodic routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. This type of routing requires each node to periodically broadcast the network topology of its own view so that every node in the network can maintain one or more routing tables to store up-to-date routing information. The destination-sequenced distance-vector (DSDV) routing protocol is a periodic protocol based on the classical Bellman-Ford routing mechanism. The use of destination sequence number for each routing update is to prevent from loops in routing tables.

On-demand routing protocols:

A different approach from periodic approach is the source-initiated on-demand routing. This type of routing establishes routes on an as-needed basis. When a node requires a route to some node in the network, it initiates a route discovery process. Once a route has been established, it is maintained by a route maintenance procedure until it no longer appears to be useful. One example of on-demand routing is the Ad hoc on-demand distance vector (AODV) routing protocol. When a node desires to send a message to some destination node and does not already have a valid route to that node, it broadcasts a route request (RREQ) packet to its neighbours. When a node receives the RREQ packet, it checks if there is a fresh enough route to the destined node. If so, it replies to the RREQ by sending a route reply (RREP) in return; otherwise, it forwards the RREQ to its neighbours. If no intermediate node has fresh enough route, the RREQ will eventually reaches the destination node which then replies an RREP to the source node. As the RREP is routed back along the reverse path, nodes along this path set up forward route entries in their route tables, pointing to the node from which the RREP came.

B Security in Routing Protocols

The protocols discussed above assume reliable participants; that is, all nodes are willing to cooperate. However, as ad hoc mobile wireless networks are established using wireless links, they are susceptible to hostile attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Hostile attacks may come not only from outside but from within the network. All the current proposed routing protocols for ad hoc mobile networks allow for many different types of attacks.

Some types of attacks:

- Impersonation
- Black hole
- Worm hole

Impersonation:

A malicious node may impersonate another node while sending the control packets to create an anomaly update in the routing table.

Black hole:

In this attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept

Wormhole attack:

In a wormhole attack, an attacker receives packets at one point in the network, “tunnels” them to another point in the network, and then replays them into the network from that point. For tunnelled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunnelled packet arrive sooner than other packets transmitted over a normal multi hop route.

Above attacks are common to all types of routing protocols, while other types are specific to particular routing algorithms.

For example, in AODV, a malicious node may reply to an RREQ claiming it has a fresh enough routes to the destined node but it does not really have. In DSDV, malicious node may arbitrarily tamper the update messages to disrupt the routing algorithm. Thus, security in the routing protocols is necessary in order to defend against hostile attacks.

In recent years, there have been some approaches proposed to secure routing protocols for ad hoc networks. A secure efficient ad hoc distance vector routing protocol (SEAD) based on the insecure DSDV protocol.

III OVERVIEW OF DSDV AND SEAD

A DSDV

The primary improvement for ad hoc networks made in DSDV over conventional distance vector is the addition of a sequence number in each routing table entry.

DSDV Operation:

DSDV protocol is based on the Bellman-Ford routing algorithm. In this protocol routes between the nodes in the network are always being maintained and updated. Each node in the network maintains a routing table which includes:

- The destination id.
- The next hop.
- The metric (The number of hops required to reach the destination).
- The sequence number of the information received regarding that destination.

The sequence number for each node is chosen randomly and it is usually an even number. Each node has to update its sequence number periodically and in the normal update, the sequence number is increased by two. If a node discovers an expired path and wants to send an update about it to its neighbours, only then does it increase the sequence number for a disconnected node by one. Upon receiving an update from a neighbour, a node updates an entry in its own routing table if, for that entry, the update contains a higher sequence number or the update contains a same sequence number but a shorter metric than that has been seen before. To update an entry, a node sets the metric in its table entry for that destination to one hop more than the metric in that neighbour’s update. When a node sends an update message, it puts a sequence number in the entry for itself in that update and sets the metric value to zero; for each of other entries, it duplicates all the entries maintained in its own routing table.

Advantages:

- DSDV is an efficient protocol for route discovery.
- Whenever a route to a new destination is required, it already exists at the source.
- Hence, latency for route discovery is very low.
- DSDV also guarantees loop-free paths

Disadvantages:

- DSDV needs to send a lot of control messages.
- This may generate high volume of traffic for high-density and highly mobile networks.
- A malicious node can easily disrupt the routing protocol by arbitrarily tampering the sequence numbers or the metrics.

Clearly, the sequence numbers and metric values containing in each update play a vital role in DSDV operation. Any malicious node can arbitrarily tamper the sequence number or the metrics.

So for the purpose of security protection should be provided for the sequence number and metrics. For that protection a Secure Efficient Ad hoc Distance vector (SEAD) routing protocol has been proposed will be discus in the following section.

B SEAD

To provide the security for DSDV protocol SEAD has been proposed. Secure Efficient Ad hoc distance vector routing protocol based on insecure DSDV protocol. To protect both the sequence numbers and metrics, SEAD postulates that each node maintains a one-way hash chain for its own entries in periodic updates.

Assume that the sequence numbers for a node are from 1 to the maximum value *K*, and that an upper bound *M* -1 can be placed on the diameter of the ad hoc network. Thus, within the routing protocol, all metrics in any routing update are less than M. To create a one-way hash chain, a node chooses a random initial value v_{MK} and computes $v_{MK-1}=H[v_{MK}]$, $h_{MK-2}=H[v_{MK-1}]$, …, $v_0=H[v_1]$. Where H is a one-way hash function. The group of m consecutive hash values $v_{jm}\sim v_{(j-1)m+1}$ is used to authenticate the update with sequence number *j*. The hash value v_0 is used as the authentic value that is distributed within the network.

When a node in SEAD prepares a routing update, the node includes one hash value with each entry in that update. If the node lists an entry for itself in that update, it sets the address in that entry to its own address, the metric to 0, the sequence number to its own next sequence number, and the hash value in that entry to the value relating to that sequence.

If the node lists an entry for some destination other than itself, it sets the address in that entry to that destination node's address, the metric and sequence number to the values in its routing table for that entry, and the hash value to the hash of the hash value received in the routing update entry from which it learned that route to that destination.

Upon receiving the update, a neighbour can authenticate the source node by continuously computing the hash of the value v_{mj} until obtaining a hash value belonging to the same chain that was previously disclosed.

With the use of the hash values, the sequence number can be protected since any malicious node cannot obtain legal hash value to fool its neighbours.

Disadvantages:

- When any neighbour that hears hash value sends an update, it can set the hash value to any value in the group for the sequence number *j* by doing the hash operation more than one time. This attack corresponds to arbitrarily increasing metrics. Obviously, SEAD allows for this kind of attack. For this reason, the hash chain approach in SEAD can provide authentication only for the lower bound on the metric in other router updates for that node.
- In addition, SEAD still suffers from same-distance fraud attack because when a node lists an entry for a destination, instead of placing the hash of the hash value heard from the neighbour in the entry, it may reject to do the hash operation and simply places the original hash value.

Even though SEAD has improvements over DSDV protocol it is not providing complete protection. For the purpose of complete protection secure version of DSDV (SDSDV) protocol has been proposed.

IV SDSDV PROTOCOL

In the proposed SDSDV protocol, the major goal is to protect the sequence number and the metrics in each entry of an update from being arbitrarily changed. SDSDV can guard against arbitrarily decreasing metric (including the same-distance fraud) attack and arbitrarily increasing metric attack. Thus, SDSDV can provide complete protection on the metric values.

To achieve this goal, as in SEAD we use hash chain. SDSDV postulates that each node creates two hash chains in relation to each node in the network, including itself, with one used for guarding against the decreasing metric attack and the other for against increasing metric attack. Thus, for a system with *n* nodes, each node maintains 2n hash chain.

One-Way Hash Chain:

To initialize, each node *N* forms a one-way hash chain v_{kn}, v_{kn-1},……v_0, with $v_{i-1}=H[v_i]$, where k is the maximum hop count, and n is maximum sequence number this hash chain allows. These values are used to authenticate routing update entries that specify this node *N* as a destination. To allow values v_{kn}, v_{kn-1},……$v_{1,}$ to be authenticated an authentic v_0 is published as an authenticated seed value for the node N. The value v_{ki+j} will be used to authenticate a route update entry with sequence number *i* and metric k-j for the node N as the destination when 1<=j<=k.

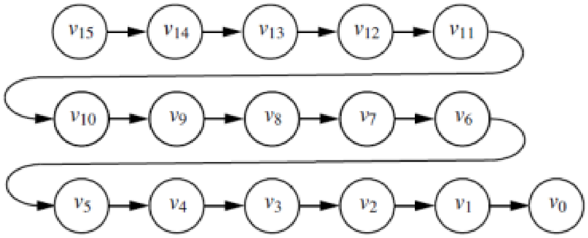

Fig: 1 Example Hash Chain, with k=5 and n=3

To initialize, *v*0 is published as an authenticated seed value for node *N*. To start the first route update for entries with *N* as the destination, the node *N* first sends *v*5 as an authenticator for sequence number 0 and metric 0. A recipient would first authenticate *v*5 using the public authenticated value *v*0, and then compute *v*4 from *v*5; the node would then advertise sequence number 0 and metric 1 using authenticator *v*4. Similarly, recipients of that update would advertise sequence number 0 metric 2 using authenticator *v*3, and so forth. The next time the node *N* starts route updates for entries with *N* as the destination, it would disclose v10 to authenticate sequence number 1 and metric 0.

Because of the properties of a one-way hash chain, a node cannot forge a routing update with higher sequence number, nor can it forge a routing update with an equal sequence number and lower metric. Larger sequence numbers take precedence over smaller ones, so nodes would simply drop updates with smaller sequence numbers, even if the metric is lower.

***Algorithm Steps*:**

To implement the SDSDV protocol algorithm as given below:

1. We use the notation $h_{x,y,m}$ and $h^1_{x,y,m}$ to denote the two chain elements *m* created by node *x* relating to node y used for guarding against decreasing metric attack and gainst increasing metric attack, respectively. These hash chains have been created using SHA-1 one way hash function.
2. To use these hash chains for authentication, we use a mechanism called Certificate Authority for a node to distribute the authentic elements from its generated hash chains.
3. Therefore, $h_{x,\ y,\ 0}$ and $h^1_{x,\ y,\ 0}$ are known to every node in the system so that they can authenticate one another within the network.
4. In addition to the destination id, the sequence number, and the metric as required in each entry in DSDV, in SDSDV will add two additional fields for each entry called AL and AC.
5. AL field is used for guarding against the decreasing attack. Entry in AL field will be done as follow:
   a. When listing an entry for itself, a node places its id number and the hash value relating to itself of current sequence number and metric 0 in the field.
   b. To list an entry for some other destination, in addition to its own id and the hash value relating to the destination node of the sequence number and current metric, an intermediate node has to place the id and the hash value received from the neighbour for that destination.
   c. As the contents of this field change from node to node we call this AL (alteration) field.
6. AC field is used for guarding against the increasing metric attack. Entry in AC field will be done as follow:
   a. To list this field, each node first copies to the field the contents of the same field in the entry for that destination received from the neighbour, and then appends its own id and the hash value relating to the destination node of the sequence number and current metric value.
   b. As the contents of this field are the accumulation of the related information of all nodes on a route, we call this field AC (accumulation) field.
7. When a node receives an entry, it verifies the hash values in AL and AC fields. If all values pass the verification, the node accepts the entry; otherwise the entry is neglected. These steps are shown in figure 2.

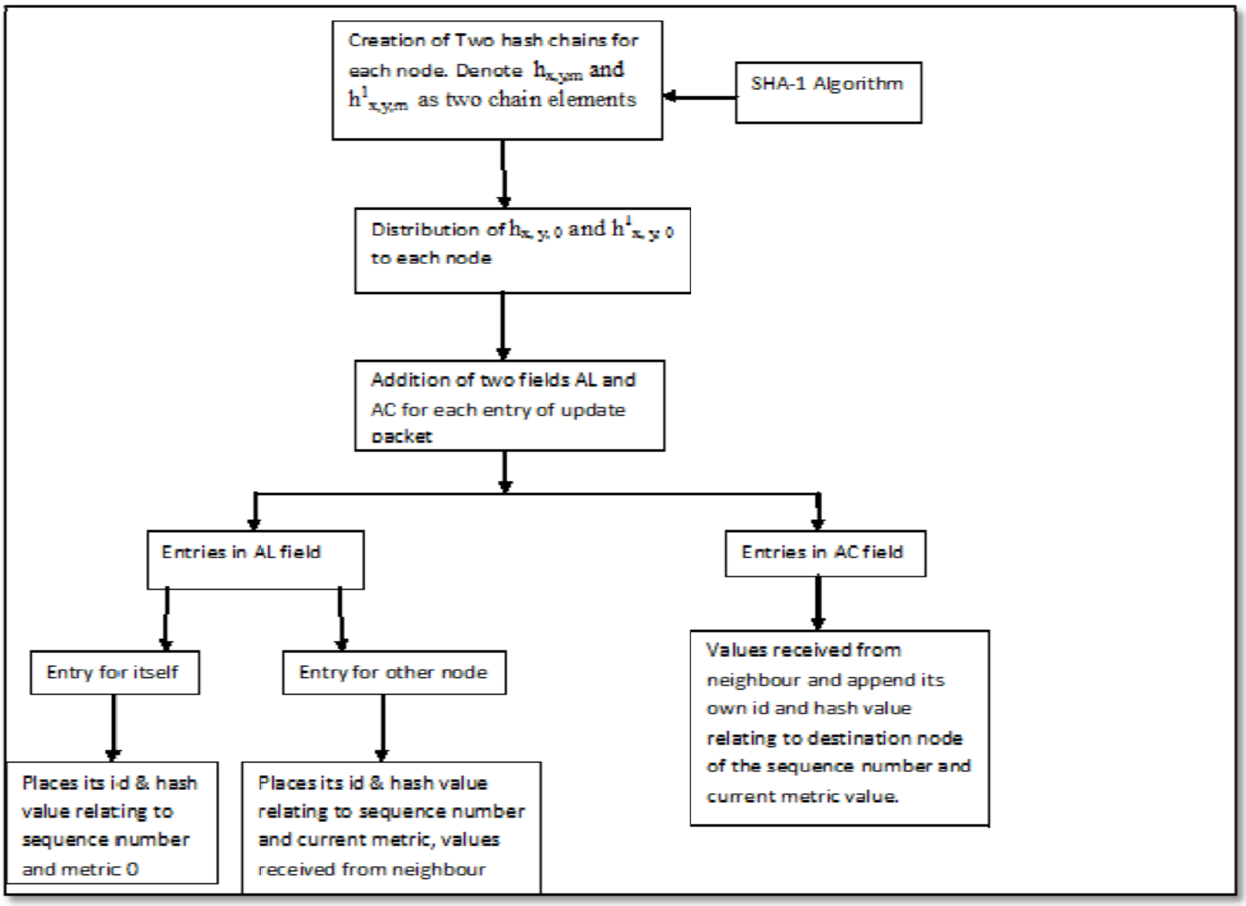
Creation of Two hash chains for each node. Denote $h_{x,y,m}$ and $h^1_{x,y,m}$ as two chain elements
SHA-1 Algorithm
Distribution of $h_{x,y,0}$ and $h^1_{x,y,0}$ to each node
Addition of two fields AL and AC for each entry of update packet
Entries in AL field
Entries in AC field
Entry for itself
Entry for other node
Values received from neighbour and append its own id and hash value relating to destination node of the sequence number and current metric value.
Places its id & hash value relating to sequence number and metric 0
Places its id & hash value relating to sequence number and current metric, values received from neighbour

Fig 2: SDSDV Protocol

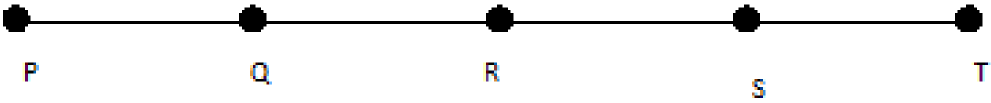

Figure 3: simple network

We now illustrate how these two fields can be used to protect the metric values from maliciously tampering by way of the following example. Consider the topology of a simple network shown in Fig. 3, where several nodes are on a line and each node can hear only its neighbour(s). Suppose node P attempts to send an update of sequence number *j*. In SDSDV protocol entries for AL and AC fields have been made for corresponding sequence number. Table 1 lists the contents of the AL and AC fields in the entries with node P as a destination transferred from node P to node S.

TABLE 1: CONTENTS OF THE AL AND AC FIELDS

Sender -> Receiver	Fields	Content of fields
P → Q	AL field	P's id & $h_{P,P,jm}$
	AC field	P's id & $h^1_{P,P,jm}$
Q→ R	AL field	P's id & $h_{P,P,jm}$ Q's id & $h_{Q,P,jm-1}$
	AC field	P's id & $h^1_{P,P,jm}$ Q's id & $h^1_{Q,P,jm-1}$
R→ S	AL field	Q's id & $h_{Q,P,jm-1}$ R's id & $h_{R,P,jm-2}$
	AC field	P's id & $h^1_{P,P,jm}$ Q's id & $h^1_{Q,P,jm-1}$ R's id & $h^1_{S,P,jm-2}$

V CONCLUSION

MANETS giving an emerging wireless networking technology for future mobile communications. Therefore the design of routing protocols for such networks is more challenging than that for wired networks. A secure DSDV protocol (SDSDV) for MANETS, as a manner similar to SEAD, uses the hash chain approach to securing the sequence numbers and metrics. One-way hash chains are a frequently used cryptographic primitive in the design of secure protocols. SDSDV postulates that each node creates two hash chains in relation to each node in the network, including itself, with one used for guarding against the decreasing metric attack and the other for against increasing metric attack. Thus, for a system with *n* nodes, each node maintains 2n hash chains. With use of the AL and AC fields in the entry, any nodes in SDSDV in a route cannot arbitrarily increase or decrease the sequence number and metric. Thus, the SDSDV can provide a complete protection on the routing messages.

VI. REFERENCES

1. http://www.it.iitb.ac.in/~abhiseth/seminar.pdf
2. C. E. Perkins, ed., *Ad Hoc Networking*, Addison-Wesley, 2001.
3. E. M. Royer and C-K Toh, "A review of current routing protocols for ad hoc mobile wireless networks," *IEEE Personal Comm.*, pp. 46–55, April 1999.
4. C. E. Perkins and P. Bhagwa, "Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers," *Comp. Commun. Rev.*, pp. 234–244, Oct. 1994.
5. H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *IEEE Commun. Mag.*, pp. 70–75, Oct. 2002.
6. Y-C Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," *Ad Hoc Networks*, pp. 175–192, Vol.1, 2003.
7. L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, pp. 24–30, Nov./Dec. 1999.
8. Y-C Hu, A. Perrig, and D. B. Johnson, "Ariadn: A secure on-demand routing protocol for ad hoc networks," In *Proceedings MobiCom'02*, 23–26, Sept. 2002.
9. P. Papadimitrators and Z. J. Haas, "Secure routing for mobile ad hoc networks," In *Proceedings CNDS 2002*, 27–31, Jan. 2002.
10. K. Sanzgiri, et al., "A secure routing protocol for ad hoc networks," In *Proceedings 10th IEEE ICNP*, pp. 78–89, 2002.
11. Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless ad hoc networks," In *Proceedings IEEE Infocomm 2003*, April 2003.