Providing Security using Hash Algorithm for Chanel Aware Routing in MANET'S

R.Sandeep Kumar[1], M.Venkata Krishna Reddy [2] , D.Jamuna[3]

Dept. Computer Science & Engineering JPNCE, Mehaboob Nagar.

Abstract
A Mobile Ad-hoc Network (MANET) is a collection of autonomous nodes or terminals which communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner. Nodes in ad-hoc networks play both the roles of routers and terminals. Moreover, the routing path in ad-hoc networks is dynamic; it is not fixed as in wired networks. Therefore, some security mechanisms used in wired networks cannot simply be applied to protocols in ad-hoc networks. After analyzing various types of attacks against ad-hoc networks, a secure scheme for the famous routing protocol, CA- AOMDV (Channel Aware ad hoc multipath distance vector routing) is proposed. To guarantee the integrity in ad-hoc networks, Secure Hash Algorithm-1 (SHA-1) is used. Furthermore, NS2 (Network Simulator) software is used to simulate this scheme and performance analysis are made.

Index Terms
mobile ad hoc networks, channel aware routing, security, SHA1

1. Introduction

In a multi-hop mobile ad-hoc network, mobile nodes cooperate to form a network without using any infrastructure such as access points and base stations. Instead, the mobile nodes forward packets for each other's allowing communication among nodes outside wireless transmission range. Examples of applications for ad-hoc networks range from military operation and emergency disaster relief to community networking and interaction among meeting attendees or students during a lecture. In this ad-hoc networking applications, security is necessary to guard the network from various types of attacks. In ad-hoc networks, adverse nodes can freely join the network, listen to and/or interfere with network traffic, and Compromise network nodes leads to various network failures. Since routing protocols are fundamental tools of network-based computation, at tacks on unsecured routing protocols can disrupt network performance and reliability.

2. review of aomdv and ca-aomdv

Transmissions via unreliable wireless connections can result in large packet losses. Thus, it makes sense to consider routing protocols which adapt to channel variations. We use a channel-aware routing protocol which extends the Ad hoc On- Demand Multipath Distance Vector (AOMDV) routing protocol. We call it CA-AOMDV. AOMDV is, itself, an extension of the Ad hoc On-Demand Distance Vector (AODV) routing protocol. In this section, we review the details of these two predecessor protocols that are useful to our discussion in this paper. AOMDV the key distinguishing feature of AOMDV over AODV is that it provides multiple paths to nd. These paths are loop free and mutually link-disjoint. AOMDV uses the notion of advertised hop-count to maintain multiple paths with the same destination sequence number. In both AODV and AOMDV, receipt of a RREQ initiates a node route table entry in preparation for receipt of a returning RREP.

AOMDV and CA-AOMDV routing table structure

AOMDV ROUTING TABLE	CA-AOMDV ROUTING TABLE
Destination IP address	Destination IP address
Destination sequence number	Destination sequence number
Advertised hop count	Advertised hop count
Path list { (next hop IP1,hopcount 1), (next hop IP2,hop	Dmin
	Path list { (next hop IP1,hopcount 1,d1),
count 2)….}	(next hop IP2,hop count 2, d2)…..}
Expiration time	Expiration time
	Dormant time

In AODV, the routing table entry contains the fields:
<destination IP address, destination sequence number, next-hop IP address,
hop-count,
entry expiration time>,
where entry expiration time gives the time after which, if a corresponding RREP has not been received, the entry is discarded. In AOMDV, the routing table entry is slightly modified to allow for maintenance of multiple entries and multiple loop- free paths. First, advertized hop-

Manuscript received August 5, 2013
Manuscript revised August 20, 2013

count replaces hop- count and advertized hop-count is the maximum over all paths from the current node to nd, so only one value is advertized from that node for a given destination sequence number. Second, next-hop IP address is replaced by a list of all next-hop nodes and corresponding hop-counts of the saved paths to nd from that node, as follows:
<destination IP address, destination sequence number, advertized hop-count, route list:
{(next hop IP 1, hop-count 1),
(next hop IP 2, hop-count 2), . . . },
entry expiration time>.

To obtain link-disjoint paths in AOMDV, nd can reply to multiple copies of a given RREQ, as long as they arrive via different neighbors.

3. route discovery in ca-aomdv

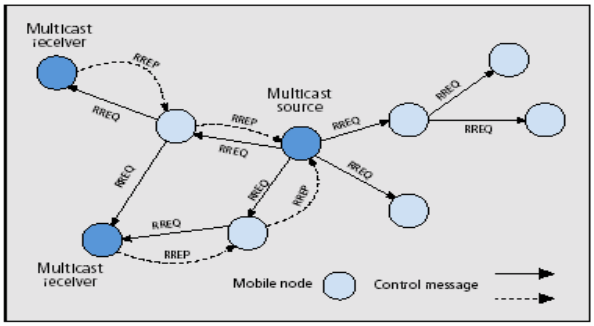
Route discovery in CA-AOMDV is an enhanced version of route discovery in AOMDV, incorporating channel properties for choosing more reliable paths. we defined the ANFD for one link of a path, according to the mobile-to-mobile channel model. CA-AOMDV uses the ANFD as a measure of link lifetime. The duration, D, of a path is defined as the minimum ANFD over all of its links,

$$\mathcal{D} \triangleq \min_{1 \le h \le \mathcal{H}} \mathrm{ANFD}_h,$$

Where h is link number, and H is number of links/hops in the path. Before forwarding a RREQ to its neighbors, a node inserts its current speed into the RREQ header so that its neighbors can calculate the link ANFD using (1). The path duration, D, is also recorded in the RREQ, updated, as necessary, at each intermediate node. Thus, all information required for calculating the ANFD is available via the RREQs , minimizing added complexity. Similarly, to the way the longest hop path is advertised for each node in AOMDV to allow for the worst case at each node, in CA-AOMDV the minimum D over all paths between a given node, ni, and nd, is used as part of the cost function in path selection. That is,

$$\mathcal{D}_{\min}^{i,d} \triangleq \min_{\zeta \in \mathrm{path\_list}_i^d} \mathcal{D}_\zeta,$$

where path list di is the list of all saved paths between nodes ni and nd. The route discovery update algorithm in CA-AOMDV is a slight modification of that of AOMDV. If a RREQ or RREP for nd at ni, from a neighbor node, nj, has a higher destination sequence number or shorter hop- count than the existing route for nd at ni, the route update criterion in CA-AOMDV is the same as that in AOMDV. However, if the RREQ or RREP has a destination sequence number and hop-count equal to the existing route at ni but with a greater Di;d min, the list of paths to nd in ni's routing table is updated. So, in CA-AOMDV, path selection is based on Di;d min as well as destination sequence number and advertised hop-count. The routing table structures for each path entry in AOMDV and CA- AOMDV are shown in Table 1. The handoff dormant time field in the routing table for CA-AOMDV is the amount of time for which the path should be made dormant due to channel fading. It is set to the maximum value of the AFDs over all links in the path. This use of handoff dormant time is described in more detail in the next section.



Route discovery in CA-AOMDV

4. route maintenance

When a source node broadcasts an RREQ for a multicast group, it often receives more than one reply. The source node keeps the received route with the greatest sequence number and shortest hop count to the nearest member of the multicast tree for a specified period of time, and disregards other routes. At the end of this period, it enables the selected next hop in its multicast route table, and unicasts an activation message (MACT) to this selected next hop. The next hop, on receiving this message, enables the entry for the source node in its multicast routing table. If this node is a member of the multicast tree, it does not propagate the message any further. However, if this node is not a member of the multicast tree, it would have received one or more RREPs from its neighbors. It keeps the best next hop for its route to the multicast group, unicasts MACT to that next hop and enables the corresponding entry in its multicast route table. This process continues until the node that originated the chosen RREP (member of tree) is reached. The activation message ensures that the multicast tree does not have multiple paths to any tree node.

5. standard security services

The following are the standard security services.

1. Data Confidentiality: It is the property in which the information embedded in network traffic is prevented from unauthorized disclosure. Since one of the main reasons that an attacker an successfully attack network nodes and protocols is the leak of sensitive information such as passwords and configuration data, data confidentiality is a very important property of network security.
2. Data Integrity: It is the property in which the originality of the information transmitted over the network is ensured. It is often combined with data origin authentication since data integrity alone cannot help receivers decide whether the received data are forged or have been tampered with.
3. Authentication: It is the property in which the identity of the connected entity (node) can be confirmed during connection phase (i.e., peer entity authentication), and the source of a message transmitted during the data transfer phase can be verified (i.e., data origin authentication).

A. Security in CA-AOMDV

Integrity plays an important role in ad-hoc networks. To overcome man-in-the-middle attack in mobile-ad hoc networks, SHA-1 algorithm is used. Normally, hop count field is mutable in nature. To protect this hop count value, hash values are found by using SHA- 1 algorithm for those fields. Here, the packets are sent along with the hashed values of hop count field. Now, the malicious nodes, which forward the false routing information, can be effectively defended. This algorithm takes input as source address, destination address and hop count with a maximum length of less than 264 bits and produces output as a 160-bits message digest. The input is processed in 512-bits blocks. This algorithm includes the following steps.
1. Padding: The purpose of message padding is to make the total length of a padded message congruent to 448 modulo 512 (length = 448 mod 512). The number of padding bits should he between 1 and 512. Padding consists of a single 1- bit followed by the necessary number of 0-bits.
2. Appending Length: The 64-bit binary representation of the original length of the message is appended to the end of the message.
3. Initialize the SHA-1 buffer: The 160-bit buffer is represented by five four-word buffers (A, B, C, D, E) used to store the middle or finally results of the message digests for SHA-I functions and they are initialized to the following values in hexadecimal. Low-order bytes are put
Word A: 67 45 23 01
Word B: EF CD AB 89
Word C: 98
BA DC EF
Word D: 10
32 54 16
Wnrd E: C3 D2 El FO
.
..
4. Process message in 16-word blocks: The heart of the algorithm is a module that consists of four rounds of processing 20 steps each. The four rounds have a similar structure, but each uses a different primitive logical function.
These logical functions are defined as follows:
Initialize hash value: a: =A, b: =B, c: =C, d=: D, e=:E Main loop:
for I from 0 to 79 if 0 _ i _ 19 then
f := (b and c) or((not b) and d)
k := 0x5A827999 else if 20 _ i _ 39
f := b xor c xor d k:=0x6ED9EBA1
else if 40 _ i _ 59
f := (b and c) or (b and d) or (c and d)
k := 0x8F1BBCDC
else if 60 _ i _ 79
f := b xor c xor d
k := 0xCA62C1D6
The output of the fourth round is added to the input of the first round, and then the addition is modulo 232 to produce the ABCDE value that calculate next 5l2- bits block.
5. Output: After all 512-bits blocks have been
processed, the output of the last block is the 160- bits message digest. These message digest values are sent along with the packets .
So, the packets which are sent by malicious nodes are suppressed. Thus, the integrity is ensured.

B. Secured CA-AOMDV Route Discovery algorithm
Sender Generates RREQ packet;

Sender signs all non-mutable fields (except hop count and hash chain fields) with its private key; Apply Hash to a seed to generate hash chain field; if (intermediate node can reply)
{Clear destination only tag; Include second signature in the signature extension;
}
Append signature extension to RREQ packet;
Broadcast RREQ to all neighbor nodes;
Intermediate node receives RREQ packet;
Node Verifies signature with public key of source (from RREQ packet);
If (valid packet)
then
update routing information of
source in any (establishment of reverse path);
if (destination I.P == node I.P)
{
Generate RREP;
Sign all the signs all non-mutable fields
(except hop count and hash chain fields)
with its private key;
Apply Hash to a seed to generate hash chain field;

Append signature extension to RREP
packet;
Unicast RREP to the neighbor which is in the reverse path for the source node;
}
else if (Node has valid route for destination &&
! (Destination only tag))
{
Generate RREP;
Copy the signature and other necessary
field of source to the signature extension; Sign all the signs all non-mutable fields (except hop count and hash chain fields) with its private key;
Apply Hash to a seed to generate hash chain field;
Append signature extension to RREP
packet;
Unicast RREP to the neighbor which is in the reverse path for the source node;
}
else

6. simulation

For simulation, we used network simulator ns-2.34, implementing the mobile-to=-mobile channel with Doppler frequency. This model has considered an area of 750m X 750m with a set of mobile nodes placed randomly and broadcast range is 150m.The simulation was carried out for different number of nodes using Network simulator (NS2).

A. Simulation Results
Here, we consider 25 mobile nodes with Channel aware routing protocol with the following parameters.

Table 2. Simulation Parameters.

Routing Protocol	CA-AOMDV
No. of nodes	20
Traffic type	CBR
Channel capacity	2 Mbps
Simulator	NS2
CBR packet size	512 bytes

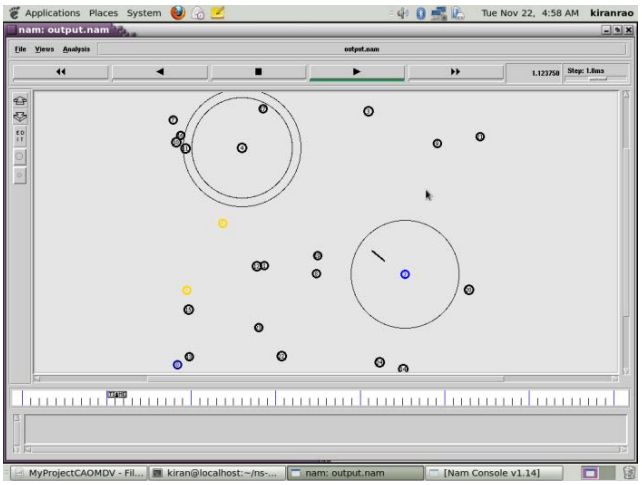


Figure 1 shows data transmission between source and destination node without malicious nodes

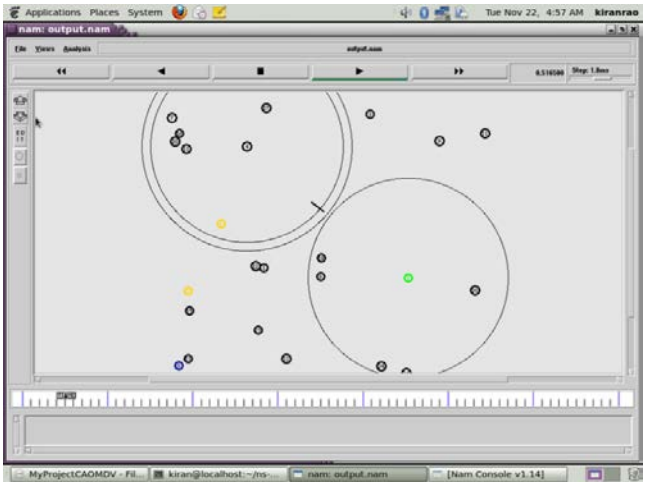
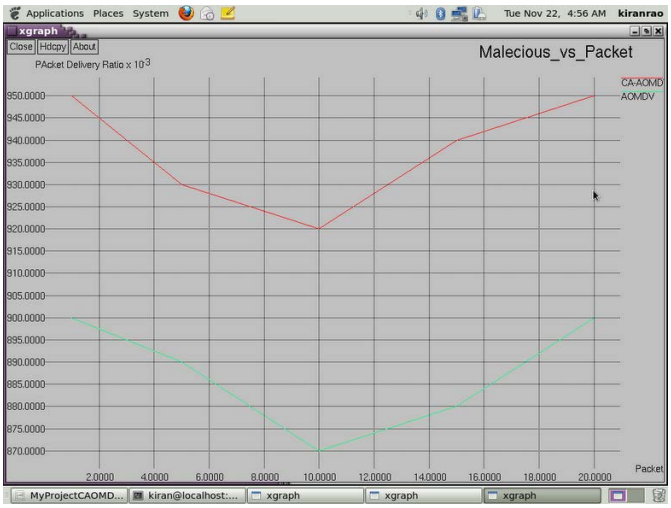


Figure2 shows data transmission with malicious nodes.



Secured CA-AOMDV Packet Delivery ratio

7. conclusion and future work

The purpose of this paper is to find an efficient and secure communication in wireless ad- hoc networks. Here, SHA-1 algorithm is applied in CA-AOMDV protocol to achieve secure routing in MANET. CA-AOMDV is used to generate stable link between source and destination. There are still many problems such as tunneling attacks, selectively drop packets; etc are still persist in these ad-hoc networks.

References

[1] Xiaoqin Chen, Haley M. Jones, and Dhammika Jayalath, "Channel-Aware Routing in MANETs with Route Handoff" IEEE Transactions on Mobile computing, VOL. 10. NO. 1, JANUARY 2011.
[2] Mr.P.VISU, Mr.W.T.CHEMBIAN, Mr.S.KOTEESWARAN"Security in Multicast Mobile Ad-hoc Networks" IEEE 2009.
[3] S.Biswas and R.Morris, "ExOR: opportunistic MultiHop Routing for wireless Networks", vol. 35,no. 4, pp. 133-144 Aug.2005
[4] Dai Zibin and Zhou Ning, "FPGA Implementation of SHA-1 Algorithm", IEEE 2003, pp 1321-1324.
[5] Junaid Arshad and Mohammad Ajmal Azad, "Performance Evaluation of Secure on- Demand Routing Protocols for Mobile Adhoc Networks", IEEE Network, 2006, pp 971- 975.
[6] A.S. Akki, "Statistical Properties of Mobile-to-Mobile Land Communication Channel," IEEE Trans. Vehicular Technology, vol. 43, no.4, pp. 826-831, Nov. 1994.
[7] N. Priyantha, A. Miu, H. Balakrishnan, and S.Teller, "The Cricket Compass for Context-Aware Mobile Applications," Proc. ACMMobiCom, pp. 1-14, July 2001.
[8] T. Goff, N. Abu-Ghazaleh, D. Phatak, and R.Kahvecioglu, "Preemptive Routing in Adhoc Networks," Proc. Ann. Int'l Conf. Mobile Computing and Networks (ICMCN), pp.43-52, July 2001.
[9] [The Network Simulator - ns-2, http://www.isi.edu/nsnam/ns, 2008.
[10] C.S. Patel, G.L. Stuber and T.G. Pratt, "Simulation of Rayleigh- Faded Mobile-to-Mobile Communication Channels," IEEE Trans. Comm., vol. 53, no. 11, pp. 1876-1884, Nov. 2005.

First Author R.Sandeep Kumar Studying MTech in CSE Dept. Jayaprakash Narayan College of Engineering, Mahabubnagar. Andhra Pradesh INDIA B.Tech (CSE) from Sri Kottam Tulasi Reddy Memorial College of Engineering, Gadwal

Second Author – M. Venkata Krishna Reddy, Working as Assoc. Professor in CSE Dept. Jayaprakash Narayan College of Engineering(JPNCE), Mahabubnagar, MTech(CSE) from Vidya Vikas Institute of Technology, Hyderabad. B.Tech (CSE) from Sri Kottam Tulasi Reddy Memorial College of Engineering, Gadwal. His areas of Interest are in Mobile Adhoc Networks, Data Mining, Networking and guided M. Tech and B. Tech Students IEEE Projects.

Third Author- Prof.D.Jamuna, Working as Professor & Head of CSE Dept. Jayaprakash Narayan College of Engineering, Mahabubnagar, M.Tech (SE) from School of Information Technology, JNTUH, Hyderabad. BE (CSE) from Vijayanagara Engineering College, Bellary. Experience 15 Years in Teaching Profession. Her areas of Interest are in Wireless Sensor Networks, Data Mining, Networking and guided M. Tech and B. Tech Students IEEE Projects. She is a Member of CSI