A Novel Authenticated Digital Watermarking in Mobile Ad-hoc Networks Using ns-2 Simulator

Mehemed Bashir Aliwa[†], **Tark El-Ahmady El-Tobely**[†], **Mahmood M. Fahmy**[†], **Mohamed EL Said Nasr**[†] **and Mohamed Hashem Abd El-Aziz**[††]

[†]Faculty of Engineering-TANTA University, Egypt.

[††]Faculty of Computers & Information Sciences-Ain Shams University, Egypt.

Summary

Mobile ad-hoc networks MANETs are extensively used in defense and rescue applications. The dynamic topology of MANETs allows nodes to join and leave the network at any point of time. This dynamic property has rendered it vulnerable to various security attacks than traditional wired networks. Many solutions have been proposed in recent researches for secure routing protocol to increase the security of MANETs. In this paper, have been proposed and evaluate a novel authenticated digital watermarking algorithm in mobile ad-hoc distance vector routing protocol (AWDV) based on the design of the Destination-Sequenced Distance-Vector routing protocol DSDV. In order to support use with nodes to guard against Byzantine and Denial-of-Service attacks attempts to cause other nodes to consume excess network bandwidth or processing time, have been used to embed a watermark bits in each routing advertisements to create authentic watermarked packet entry in an routing update. The result of the AWDV proposed was compared with the standard DSDV and secure efficient ad-hoc distance vector routing protocol SEAD under the performance analysis of simulation setup ns-2 and metrics. The results obtained prove that the proposed AWDV outscores the traditional DSDV and SEAD in all aspects. The proposed AWDV enhanced table-driven DSDV provides the solution for the possible packet dropping attack in an ad-hoc network.

Key words:

Mobile ad-hoc network, digital watermarking, routing protocol, attacker, ns-2 simulator and performance metrics.

1. Introduction

The MANET is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration[1][2]. Ad-hoc networks all nodes are mobile and can be connected dynamically in an arbitrary manner. All nodes of these networks behave as routers and take part in discovery and maintenance of routes to other nodes in the network. MANET's are very useful in tactical military, emergency search, disaster relief, sensor, rescue operations, conferences and meetings or conventions in which persons wish to quickly share information[33]. There are a number of characteristics in MANET's. Dynamic topologies, bandwidth constrain, energy-constrained and limited physical security[4][6], the two different types of attacks in MANETs can be disrupted in routing function by external (passive) or internal (active) attacks[4][7]. An external attacker does not disrupt the operation of the routing protocol, but tries to discover valuable information by monitoring the traffic, for an internal attacker is that it is able to injects false routing information and tries to disrupt the operation of the protocol in order to limit availability, gain authentication, or divert packets. So that the internal attackers have the capabilities of the strongest outside attacker, as they are legitimate participants of the routing process. Having complete access to the communication link they are able to advertise false routing information at will and force arbitrary routing decisions on their peers. One of the most difficult to detect problems in routing is that of Byzantine failures[17]. These failures are the result of nodes that behave in a way that does not comply with the protocol[9], the specific attacks that can target the operation of a routing protocol in MANET:

Byzantine attack, a compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services[7].

Denial-of-Service attacks 'DoS', an attacker attempts to cause other nodes to consume excess network bandwidth or processing time[11].

Impersonation or spoofing attack, since current ad-hoc routing protocols do not authenticate routing packets[24]. It is the misrepresentation of the network topology that may cause network loops or partitioning.

Routing table overflow attacker, attempts to create routes to nonexistent nodes. The goal is to have enough routes so that creation of new routes is prevented or the implementation of routing protocol is overwhelmed.

- Replay attack, an attacker sends old advertisements of routing information to a node causing it to update its routing table with stale routes[10].

Manuscript received April 5, 2011
Manuscript revised April 20, 2011

- Modification attacks, malicious nodes can easily modifying routing information[7] and attacker can cause network traffic to be dropped, be redirected to a different destination, or take a longer route to the destination, thus increasing communication delays.
- The organization of the rest paper is as follows: In section.2 the problem definition, in section.3 described the routing protocols in MANETs and in section.4 the proposed a novel authenticated digital watermarking routing protocol. In section.5 the performance analysis of proposed AWDV algorithm described simulation setup, performance metrics and experimental results with discussion. Finally, conclusion and future work.

2. Problem Definition:

In this paper the problem statement in MANETs one of the major concerns is how to increase the routing security in presence of malicious nodes. Where the dynamic topology of MANET's allows nodes to join and leave the network at any point of time. This dynamic property of has rendered it vulnerable to various security attacks[10][31]. Whereas the existing link level security techniques (e.g. encryption) are often applied within wireless networks to reduce these threats[4]. Absent link level security, at the network layer, the most pressing issue is one of inter-router authentication prior to the exchange of network control information, due to the dynamic changes of topology; it is difficult to determine whether the node participating in the routing domain is Byzantine or DoS attacks, then indeed an authenticated node. However the security requirements of MANET's are route signaling can't be spoofed, fabricated routing messages can't be injected into the network, routing messages can't be altered in transit, routing loops can't be formed by through malicious action, routes can't be redirected from the shortest path by malicious action and unauthorized nodes should be excluded from route computation and discovery[4].

The digital watermarking solutions can be employed to prevent the impact of external attackers by mutual authentication of the participating nodes through authenticated digital watermarking in spatial domain scheme[21][22][23]. A digital watermarking is used to insert an imperceptible signal into digital data[16], it has a variety of applications like copyright control, authenticity,…etc[12]. Watermark is used to provide authentication like the ID cards[13]. It may be designed in such a way that, any possible alteration in the data either destroys the watermark or creates a mismatch between the content and the watermark that can easily be detected[12]. Moreover the digital watermarking differs from cryptography, where cryptography is the art of sending a message by converting it into a secret code called as cipher text, here, the very existence of the message is not being kept secret but only the contents are, this rouses suspicion and curiosity. But the digital watermarking, unlike cryptography, leaves the original medium or data almost unaltered even after embedding it with the copyright information. The naked eye cannot tell the difference in the alteration and machine inspection[13][14][15]. We aim at introducing to development an enhanced approach for authenticated digital watermarking in MANET that is satisfies these requirements and problems at the same time in an acceptable manner.

3. Routing Protocols in MANETs

There are a number of routing protocols have been developed for MANET's. They can be divided into three categories[4][9] (Flat, Hierarchical, Geographic position assisted) routing: the flat routing can be divided into proactive (the table-driven) and reactive (the source-initiated on-demand) protocols[11][25]. The Destination Sequenced Distance Vector Routing protocol (DSDV) belongs to the table-driven protocols[8]. The most popular protocols nowadays are Dynamic Source Routing protocol DSR[34] belong to the source-initiated on-demand protocols. We will briefly describe distance vector routing DV, DSDV routing protocol in MANET's and SEAD secure routing protocol in MANET's are the following:

A. Distance Vector Routing

In DV routing[8][25], each router maintains a routing table listing all possible destinations within the network. Each entry in a node's routing table contains the address (identity) of some destination, this node's shortest known distance (usually in number of hops) to that destination, and the address of this node's neighbor router that is the first hop on this shortest route to that destination; the distance to the destination is known as the metric in that table entry. Each router forwarding a packet uses its own routing table to determine the next hop towards the destination. To maintain the routing tables, each node periodically broadcasts routing update containing the information from its own routing table. Each node updates its own table using the updates it hears, so that its route for each destination uses as a next hop the neighbor that advertised the smallest metric in its update for that destination; the node sets the metric in its table entry for that destination to '1' (hop) more than the metric in that neighbor's update[18][20].

B. DSDV

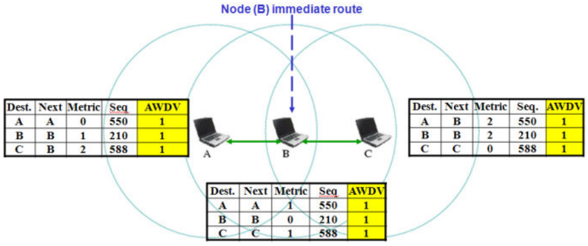
The DSDV routing protocol[8][25] is a table-driven algorithm based on the classical Bellman-Ford routing mechanism[19]. Every mobile node in the network maintains a routing table in which all of the possible destinations within the network and the number of hops to each destination are recorded. Each entry is marked with a sequence number assigned by the destination node. The sequence numbers enable the mobile nodes to distinguish stale routes from new ones, thereby avoiding the formation of routing loops. Routing table updates are periodically transmitted throughout the network in order to maintain table consistency. In order to reduce the amount of information carried in these packets, two types will be defined. One will carry all the available routing information, called a "full dump". The other type will carry only information changed since the last full dump, called an "incremental". First the full dump. This type of packet carries all available routing information and can require multiple network protocol data units NPDUs. During periods of occasional movement, these packets are transmitted infrequently. Second Smaller incremental packets are used to relay only that information which has changed since the last full dump. Each of these broadcasts should fit into a standard-size NPDU, thereby decreasing the amount of traffic generated. The mobile nodes maintain an additional table where they store the data sent in the incremental routing information packets. New route broadcasts contain the address of the destination, the number of hops to reach the destination, the sequence number of the information received regarding the destination, as well as a new sequence number unique to the broadcast. The route labeled with the most recent sequence number is always used. In the event that two updates have the same sequence number, the route with the smaller metric is used in order to optimize (shorten) the path. Mobiles also keep track of the settling time of routes, or the weighted average time that routes to a destination will fluctuate before the route with the best metric is received. By delaying the broadcast of a routing update by the length of the settling time, mobiles can reduce network traffic and optimize routes by eliminating those broadcasts that would occur if a better route was discovered[1][17][24].

C SEAD

Secure Efficient Ad-hoc Distance vector routing protocol (SEAD)[18] is a part of the Destination-Sequenced Distance-Vector ad-hoc network routing protocol. The SEAD use efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol. 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 a fixed-length bit string. Thus, $H:\{0,1\}^* \rightarrow \{0,1\}p$, where ρ is the length in bits of the hash output.. The function H should be simple to compute yet must be computationally infeasible in general to invert. To create a one-way hash chain, a node chooses a random $x \in \{0,1\}\rho$ and computes the list of values h0, h1, h2, h3,…, hn, where h0=x, and hi = H(hi-1) for $0< i \leq n$, for some n. The node at initialization generates the elements of its hash chain as shown above, from "left to right" (in order of increasing subscript i) 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" (in order of decreasing subscript i) within the generated chain. Given an existing authenticated element of a 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 of decreasing subscript). For example, given an authenticated hi value, a node can authenticate hi-3 by computing H(H(H(hi-3))) and verifying that the resulting value equals hi. To use one-way hash chains for authentication, we assume some mechanism for a node to distribute an authentic element such as hn from its generated hash chain. Authenticating routing updates each node in SEAD uses a specific single next element from its hash chain in each routing update that it sends about itself (metric '0'). Based on this initial element, the one-way hash chain conceptually provides authentication for the lower bound of the metric in other routing updates for this destination; the authentication provides only a lower bound on the metric. We assume that an upper bound can be placed on the diameter of the ad hoc network, and we use (m-1) to denote this bound. The method used by SEAD for authenticating an entry in a routing update uses the sequence number in that entry to determine a contiguous group of m elements from that destination node's hash chain, one element of which must be used to authenticate that routing update. The particular element from this group of elements that must be used to authenticate the entry is determined by the metric value being sent in that entry. Specifically, if a node's hash chain is the sequence of values h0, h1, h2, h3,…,hn and n is divisible by m, then for a sequence number i in some routing update entry, let k=((n/m)-i). An element from the group of elements hkm, hkm+1,…,hkm+m-1, from this hash chain is used to authenticate the entry; if the metric value for this entry is j, $0\leq j < m$, then the value hkm+j here is used to authenticate the routing update entry for that sequence number. Nodes receiving any routing update can easily authenticate each entry in the update, given any earlier authentic hash element from the same hash chain[20].

4. Proposed A Novel Authenticated Digital Watermarking Routing Protocol

In this section, have been proposed a novel authenticated digital watermarking algorithm in mobile ad-hoc network by modifying the destination sequenced distance vector routing protocol DSDV[1][8][17][25] used to embed watermark bits in each authentic routing advertisements to create authentic watermarked packet entry in an routing update, whereas the mobile nodes maintain an additional table with new table entry of authentic route (AWDV) value as shown in Fig.1are store the data sent or received in the incremental authentic routing information packet. A new authentic route broadcasts contain the address of the destination, the number of hops to reach the destination, the sequence number of the information received regarding the destination with watermarked packet, as well as the authentic routing update can be generate by employ smaller incremental packet is used to relay only that information which has changed and keeping track of the settling time of authentic route, for e.g. a new sequence number unique to the broadcast update, the following mechanism of authenticated digital watermarking algorithm (encoder):



Dest.	Next	Metric	Seq	AWDV
A	A	0	550	1
B	B	1	210	1
C	B	2	588	1

Dest.	Next	Metric	Seq.	AWDV
A	B	2	550	1
B	B	2	210	1
C	C	0	588	1

Dest.	Next	Metric	Seq	AWDV
A	A	1	550	1
B	B	0	210	1
C	C	1	588	1

Fig.1 Mobile nodes in the network maintains a routing table.

First: Each node in the topology network create randomly a numerical value matrix or gray scale image of '128' bytes in size *(a, b)* at each authentication routing advertisements. Notice that let the value $P_{(i,j)}$ be the corresponding 8 bits pair value of numerical matrix and gray scale value in the range of $0 \leq P_{(i,j)} < 2^8$.

Second: Each node in the topology network store or kept the secure watermark bits, $W \in \{0, 1\}^{\rho}$. Secret key (ρ) is the length in bits of secure watermark input is used at *encoder process* to produce authenticated routing advertisement of watermarked packet or in decoder at received authenticated routing advertisement of watermarked packet used to comparator between extracted watermark bits and original secure watermark bits to provides the successfully routing function authentication at each route advertisements.

Third: The mechanism is used for each node in the topology to distribute authenticated watermarked packet at each route advertisements, it will be using the proposed embedding algorithm[21] of an adaptively value $P_{(i,j)}$ adjustment process based on medial pyramid of embedding error by applying in falling-off-boundary in corners board set of most significant bit[22][23] with the random value manipulation in spatial domain called(APAP-MPOEE-FOBCB$_{\text{MSB6}}$)[22], *then required encoder algorithm as a step:*

<u>Step.1:</u> Extract value $P_{(i,j)}$ from created randomly a numerical matrix or image and converted into the binary bits least & most significant bit *$(LSB_{(1,2,3,4)}$ & $MSB_{(5,6,7,8)})$*, then set of the MSB_6 in each value $P_{(i,j)}$ within the boundary of corners in the first, last rows and columns of numerical matrix, when the {MSB_6 of the value $P_{(i,j)}$ = the embedded watermark bit $W_{(i,j)}$ (*EMB*)} then do nothing. Otherwise when the MSB_6 in the created value $P_{(i,j)}$ not equal the embedded watermark bit (*EMB*), it is mean that $MSB_6 \neq EMB$, thus the value $P_{(i,j)}$ can be further segmented into eight intervals is described in[22].

<u>Step.2</u>: *The pseudo code for encoder algorithm* of APAP-MPOEE$_{\text{MSBn}}$ set of the MSB_6 of the created randomly a numerical value matrix or image. Let's have a binary watermark $W_{(\rho)}$, where the bits $EMB=\{EMB_0, EMB_1, \ldots, EMB_{(k)}\}$, and set MSB_n in each value $P_{(i,j)}$of boundary in corners board, whereas $n=6$ in the range of $5 < n \leq 8$ *and* $k = 0, 1, 2, \ldots, \rho - 1$:

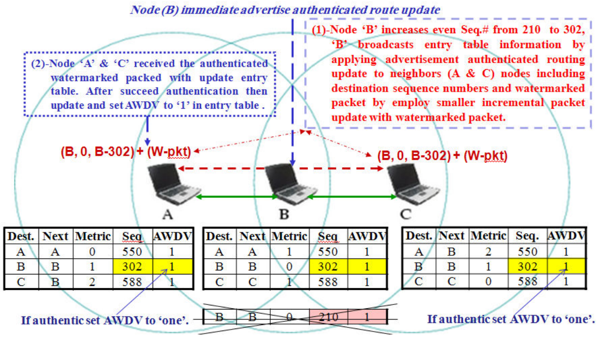
```
k = 0;
for i = 0  to  a - 1
for j = 0  to  b - 1
if($MSB_6$==0&$EMB_k$==0)|($MSB_6$==1&$EMB_k$==1),then
      "$P_{(i,j)}$ =  $P_{(i,j)}$ ;  No change.
  else if ( $MSB_6$  == 0  and  $EMB_k$ == 1 ),then
        if ( $P_{(i,j)} \geq 0$  and  $P_{(i,j)}$ <2^n-1 ), then "$P_{(i,j)}$=2^n-1;
        else  if ( $P_{(i,j)} \geq$ 2^n  and  $P_{(i,j)}$<3×2^n-1 ),then
            if ( $P_{(i,j)} \geq$ 2^n  and  $P_{(i,j)}$<5×2^n-2 ),then
              "$P_{(i,j)}$ = (2^n) -1;
            else "$P_{(i,j)}$ = 3×2^n-1; end;
          else if($P_{(i,j)} \geq$ 2^n+1  and  $P_{(i,j)}$<5×2^n-1 ),then
              if($P_{(i,j)} \geq$ 2^n+1 and  $P_{(i,j)}$<9×2^n-2 ),then
                "$P_{(i,j)}$ = (2^n+1)-1;
              else "$P_{(i,j)}$ = 5×2^n-1;   end;
            else if($P_{(i,j)} \geq$ 3×2^n and $P_{(i,j)}$<7×2^n-1 ),then
                  if($P_{(i,j)} \geq$ 3^n and $P_{(i,j)}$<13×2^n-2),then
                    "$P_{(i,j)}$ = (3×2^n)-1;
                  else "$P_{(i,j)}$  =  7×2^n-1;
                  end; end; end; end;   end;
   else if($MSB_6$== 1 & $EMB_k$== 0 ),then
         if ( $P_{(i,j)} \geq$ 2^n-1  and  $P_{(i,j)}$ <2^n ),then
         if ($P_{(i,j)} \geq$ 2^n-1  and  $P_{(i,j)}$ <3×2^n ),then
          "$P_{(i,j)}$ = (2^n-1) - 1;
          else "$P_{(i,j)}$  =  2^n;   end;
        else if ($P_{(i,j)} \geq$ 3×2^n-1  and  $P_{(i,j)}$<2^n+1),then
          if ($P_{(i,j)} \geq$ 3×2^n-1  and  $P_{(i,j)}$<7×2^n-2),then
            "$P_{(i,j)}$ = (3×2^n-1) - 1;
          else "$P_{(i,j)}$ = 2^n+1;  end;
        else if ( $P_{(i,j)} \geq$ 5×2^n-1  and  $P_{(i,j)}$<3×2^n),then
             if ($P_{(i,j)} \geq$ 5×2^n-1 and $P_{(i,j)}$<11×2^n-2),then
              "$P_{(i,j)}$  = (5×2^n-1) - 1;
            else "$P_{(i,j)}$ = 3×2^n;  end;
          else if ( $P_{(i,j)} \geq$ 7×2^n-1  and  $P_{(i,j)}$ <2^n+2 ),then
              "$P_{(i,j)}$ = (7×2^n-1)-1;
             end; end; end; end; end; end; end;
if (k < (ρ - 1))
    k = k + 1;
else  k = 0; end; end; end.
```

From the above algorithm we will applied under the algorithm FOBCB of the (a numerical value matrix or image) with the random value manipulation[23]. The proposed APAP-MPOEE-FOBCBMSB6 scheme[21][22] using to embed watermark bits in a boundary in corners board of the (image or in the first, last rows and columns of a numerical matrix), and before embedding requires a checking between the MSB6 in the boundary in corners board or matrix value P(i,j) of the created randomly (image or in the first, last rows and columns of a numerical matrix) within EMB of the embedded watermark bit, depending on the nearest of the adaptively value in the medial pyramid of embedding error to inform the forward authenticated watermarked packet value "P(i,j) obtained by a APAP-MPOEE-FOBCBMSB6 scheme.

Step.4: Decoder algorithm, the node advertises by broadcasts routing information using the mechanism of message authentication 'watermarked packet' are received by authentic route advertisement watermarked packet to neighbors node, each node required to comparator between extracted watermark bits and original secure watermark bits to provides the successfully of mechanism authentication at each route advertisements as following:

First: Extracted watermark bits from the drawbacks in FOBCB of the received 'watermarked packet' by using inverse the same procedure of the embedding algorithm without using the steps of embedding process in encoder algorithm, adjust recovery the watermark bits from the FOBCB in received 'watermarked packet' depending on the sequence number to know the manipulation value between the boundary corners board in the received 'watermarked packet' and select one of drawback from the MSB6, then the watermark in original form is thus obtained.

Second: Each node in the topology network after extracted watermark required to comparator between the extracted watermark and secure watermark to indicated in entire table of route authentication AWDV as $\in \{0,1,\infty\}$ into incremental update routing table entries at each authentic route advertisements to avoiding the formation of routing loops, where 'zero' indicate broken link, one authentic and infinite '∞' it is not authenticated, according to the install time in entire table, when entry was made (used to delete stale entries from table), where stable data pointer to a table holding information on how stable a route is used to damp fluctuations in network need to update authentication and metric number of hops to each destination or required to increase sequence number of node, for e.g. at authentic route advertisement as shown in Fig.2 a node 'B' increases even sequence number from '210' to '302', node 'B' broadcasts entry table information by applying advertise authenticated routing update to neighbors node (A & C) including address, sequence numbers of destination and number of hops (metric) with watermarked packet by employ smaller incremental packet update with watermarked packet. Then node 'A' & 'C' received the authenticated watermarked packed with update entry table. After successfully authentication routing update then set of the AWDV to '1' in entry table. Otherwise if a node is no more reachable (timeout) increase sequence number of this node by '1' (odd sequence number) and set metric = '∞' and set of AWDV to '0' in entry table. For e.g. as shown in Fig.3 at respond broken link between nodes 'C' and 'B' the node 'B' detects broken link immediately increase sequence number by '1' (only case where not the destination sets the sequence number odd number) and set of AWDV to '0' in entry table. After that immediately propagation entry table information by applying incremental advertisement authenticated routing update with watermarked packet to neighbor's node 'B' to node 'A' (if successfully routing authentication, then update information has higher sequence number and replace table entry with set of AWDV to '0').


Node (B) immediate advertise authenticated route update
(B, 0, B-302) + (W-pkt)
(B, 0, B-302) + (W-pkt)
A
B
C
If authentic set AWDV to 'one'.
If authentic set AWDV to 'one'.

(1)-Node 'B' increases even Seq.# from 210 to 302, 'B' broadcasts entry table information by applying advertisement authenticated routing update to neighbors (A & C) nodes including destination sequence numbers and watermarked packet by employ smaller incremental packet update with watermarked packet.

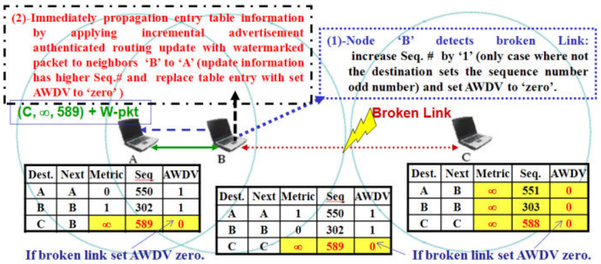
(2)-Node 'A' & 'C' received the authenticated watermarked packed with update entry table. After succeed authentication then update and set AWDV to '1' in entry table .

Dest.	Next	Metric	Seq	AWDV
A	A	0	550	1
B	B	1	302	1
C	B	2	588	1

Dest.	Next	Metric	Seq	AWDV
A	A	1	550	1
B	B	0	302	1
C	C	1	588	1
~~B~~	~~B~~	~~0~~	~~210~~	~~1~~

Dest.	Next	Metric	Seq.	AWDV
A	B	2	550	1
B	B	1	302	1
C	C	0	588	1

Fig.2 Authenticated routing advertisement update.



(2)-Immediately propagation entry table information by applying incremental advertisement authenticated routing update with watermarked packet to neighbors 'B' to 'A' (update information has higher Seq.# and replace table entry with set AWDV to 'zero')

(1)-Node 'B' detects broken Link: increase Seq. # by '1' (only case where not the destination sets the sequence number odd number) and set AWDV to 'zero'.

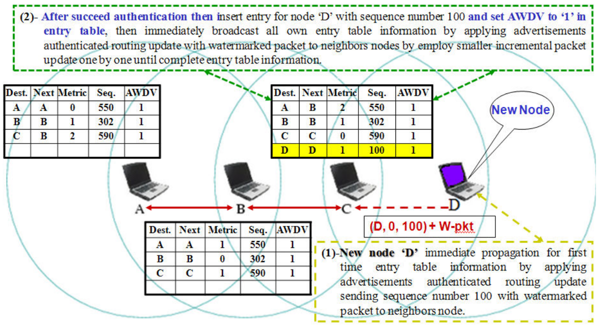
Dest.	Next	Metric	Seq	AWDV
A	A	0	550	1
B	B	1	302	1
C	B	∞	589	0

Dest.	Next	Metric	Seq	AWDV
A	A	1	550	1
B	B	0	302	1
C	C	∞	589	0

Dest.	Next	Metric	Seq.	AWDV
A	B	∞	551	0
B	B	∞	303	0
C	C	∞	588	0

Fig.3 Authenticated routing advertisement update at broken link.

In Fig.4 shows at respond to topology add new node 'D' immediate propagation for first time entry table information by applying advertisements authenticated routing update sending address and sequence numbers '100' of destination and number of hops (metric) with watermarked packet to neighbors node. After the neighbors node 'C' successfully authentication then insert entry for node 'D' with sequence number '100' and set AWDV to '1' in entry table, after finishing entry table update then immediately broadcast all own entry table information by applying advertisements authenticated routing update with watermarked packet to neighbors node by employ smaller incremental packet update one by one until completed the entry table information. Finally, Notice that after successfully routing authentication the route selection of update information is compared to own routing table select route with higher destination sequence number to ensure using newest information from destination or select the route with better metric when sequence numbers are equal.



(2)- After succeed authentication then insert entry for node 'D' with sequence number 100 and set AWDV to '1' in entry table, then immediately broadcast all own entry table information by applying advertisements authenticated routing update with watermarked packet to neighbors nodes by employ smaller incremental packet update one by one until complete entry table information.

Dest.	Next	Metric	Seq.	AWDV
A	A	0	550	1
B	B	1	302	1
C	B	2	590	1

Dest.	Next	Metric	Seq.	AWDV
A	B	2	550	1
B	B	1	302	1
C	C	0	590	1
D	D	1	100	1

Dest.	Next	Metric	Seq.	AWDV
A	A	1	550	1
B	B	0	302	1
C	C	1	590	1

(1)-New node 'D' immediate propagation for first time entry table information by applying advertisements authenticated routing update sending sequence number 100 with watermarked packet to neighbors node.

Fig.4 Respond to topology add new node.

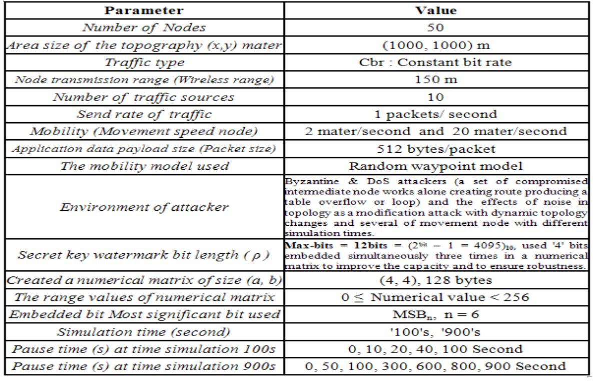
5. Performance Analysis of Proposed A Novel AWDV algorithm and Discussion

5.1. Simulation Setup

The simulation environment consists of a set of wireless and mobile networking extensions, we are using ns-2 simulator because it is a popular and powerful simulation environment, and the number of ns-2 users has increased greatly in recent years[24], that have done a simulation ns-2 studies with this environment, analyzing the behavior and performance of routing protocols and comparing it to other proposed routing protocols for ad-hoc networks[1][2][3][5][6][10][17]. The parameters used for our simulation are given in Table.1. The standard ns-2 distribution runs on Linux. However, a package for running ns-2 on Cygwin Linux Emulation for windows is available[28] the latest version of ns-2 is ns-2.34. An attempt was made to implement a novel authenticated digital watermarking algorithm in mobile ad-hoc distance vector routing protocol (AWDV) in ns-2 simulator with environment of attacker and compared with two routing protocols (SEAD and DSDV). The goal was to measure the ability of the improved proposed a novel AWDV secure routing protocol with two routing protocols to react network topology change with environment of attackers, while continuing to successfully deliver data packets to their destinations. To measure this ability, to apply a simulated network a variety of workloads, in effect testing with each data packet originated by some sender whether the routing protocol can at that time route to the destination of that packet. We are attempting to measure the performance analysis protocols on a particular performance under a range of five metrics. The routing protocols (AWDV, SEAD and DSDV) evaluations are based on the simulation of '50' wireless nodes forming an ad-hoc network, moving about over a rectangular (1000m×1000m) flat space for different simulation time as in Table.1. We chose a space in order to force the use of longer routes between nodes. In order to enable direct, fair comparisons between the protocols, it was critical to challenge the protocols with identical loads and environment attacker. Each run of the simulator accepts as input a scenario file that describes the exact motion of each node and the exact sequence of packets originated by each node, together with the exact time at which each change in motion or packet origination is to occur. We pre-generated '24' different scenario files with varying movement patterns of mobility model used random waypoint model[26][30][31] and one file traffic loads, and then ran all three routing protocols (AWDV, SEAD, and DSDV) against each of these scenario files. We run simulator ns-2 by writing the simulation code Tcl script '72' files (Tool command language) see to tutorial[26][27][32] to set up the wireless simulation components: network components types, parameters like the type of antenna, the radio-propagation model, the type of ad-hoc routing protocol, traffic models and node movement models used by mobile nodes,…etc, with movement patterns generated for '5' different pause times: 0, 10, 20, 40, and '100'seconds for simulation time 100 seconds , and '7' different pause times: 0, 50, 100, 300, 600, 800 and '900'seconds for simulation time '900'seconds , a pause time of '0' seconds corresponds to continuous motion, and a pause time of '100' (the length of the simulation) corresponds to end of stop motion at simulation time '100' seconds and as the same of simulation time 900s. Because the performance of the protocols is very sensitive to movement pattern we generated movement pattern scenario '24' files, for each value of pause time with traffic communication source model file of '10' sources as Table.1, for proposed AWDV protocol and two (SEAD and DSDV) protocols are run on the same movement patterns. We experimented with two different movement maximum speed of node. We primarily report in this paper data from simulations using two maximum node speeds of 2m/s and 20m/s. From running simulator ns-2, we generated '24' outputs trace files and animator files, for each three routing protocols (AWDV, SEAD and DSDV).

After the simulation we obtain the trace file which contains the packet dump from the simulation, where the trace files format outputs are most important files in our experiment to analyze the outputs trace file. The format of trace file for ad-hoc wireless networks depending on the packet type, the trace file may log additional information[29]. Have been implemented a Java code to extract the performance metrics from the (24×3=72) output trace files format to record the packets and compute the performance metrics graphs, also the output animator trace files can be visualized in network animator[26][27][28].

Table.1: Scenario for the simulator ns-2 experiments



Parameter	Value
Number of Nodes	50
Area size of the topography (x,y) mater	(1000, 1000) m
Traffic type	Cbr : Constant bit rate
Node transmission range (Wireless range)	150 m
Number of traffic sources	10
Send rate of traffic	1 packets/ second
Mobility (Movement speed node)	2 mater/second and 20 mater/second
Application data payload size (Packet size)	512 bytes/packet
The mobility model used	Random waypoint model
Environment of attacker	Byzantine & DoS attackers (a set of compromised intermediate node works alone creating route producing a table overflow or loop) and the effects of noise in topology as a modification attack with dynamic topology changes and several of movement node with different simulation times.
Secret key watermark bit length (ρ)	**Max-bits = 12bits** = $(2^{bit} - 1 = 4095)_{10}$, used '4' bits embedded simultaneously three times in a numerical matrix to improve the capacity and to ensure robustness.
Created a numerical matrix of size (a, b)	(4, 4), 128 bytes
The range values of numerical matrix	$0 \leq$ Numerical value < 256
Embedded bit Most significant bit used	MSB_n, n = 6
Simulation time (second)	'100's, '900's
Pause time (s) at time simulation 100s	0, 10, 20, 40, 100 Second
Pause time (s) at time simulation 900s	0, 50, 100, 300, 600, 800, 900 Second

5.2. *Performance Analysis Metrics*

In order to compare the improved proposed a novel AWDV secure routing protocol with two (SEAD and DSDV) routing protocols are run on identical movement speed and communication scenarios, studies of performance evaluations of routing protocols for MANTs indicate that the following metrics are computed for each simulation run defined:

- Packet Delivery Fraction (PDF):Which defined as the ratio of the data packets delivered to the destinations to those generated by the CBR sources and calculated as[1][2][3][5][10][17]:

$$PDF = \frac{Number\ of\ packet\ received\ by\ destination}{Number\ of\ packet\ received}$$

- Average End-to-End Delay (AED): It is a metric of data packets which includes all possible delays caused by buffering during route discovery, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times. It is very significant with real-time traffic[1][2][5][6][17]:

$$AED = \frac{\sum_{i=0}^{n} Time\ packet\ received\ - time\ packet\ sent}{Total\ number\ of\ packet\ received}$$

- Normalized Routing Load (NRL): It means that the number of routing packets transmitted per data packet delivered at the destination[1][3][6][17].

$$NRL = \frac{Number\ of\ routing\ packets\ sent}{Total\ number\ of\ packets\ received}$$

- Routing Packet Overhead (RPO): It is the total number of transmissions routing packets[1][3][17].
- Drop of Packets (DP): It is a metric to determine the amount of packets that are dropped by malicious nodes from the total dropped packets[3][10].

5.3. *Experimental Results and Discussion*

This section reports the results obtained to compare the performance of the proposed a novel AWDV routing protocol with two (SEAD & DSDV) protocols using ns-2 network simulator under the performance analysis metrics as shown in Fig.5, 6, 7, 8 and 9.

5.3.1. Packet delivery comparison

Packet delivery ratio is important as it describes the loss rate that will be seen by the transport protocols, which in turn affect the maximum throughput that the network can support. This metric characterizes both the completeness and correctness of the routing protocol.

a)- Simulation time 100s: At the lower movement speed of 2m/s, the proposed AWDV secure routing protocol performed particularly well, delivering over 95% of the data packets regardless of mobility rate as shown in Fig.5(a) with the lower movement speed of 2m/s. So for AWDV, packet delivery ratio is independent of offered traffic load, delivering between 95% and 98% of the packets at SIMT 100s, compared with SEAD delivering between 94% and 95% of the packets and DSDV delivering between 70% and 62% of the packets. The AWDV routing protocol perform better than the table-driven DSDV and SEAD protocol. Where DSDV delivering over 70% of the data packets regardless of mobility rate as shown in Fig.5(a) with the lower movement speed of (2m/s), but DSDV loses about 46% more packets than AWDV and DSDV loses about 44% more packets than SEAD at lower 10s pause times (higher mobility). Nearly all of the dropped packets are lost because a stale routing table entry directed them to be forwarded over a broken link. At the higher movement speed of 20m/s as shown in Fig.5(a), the AWDV routing protocol performed particularly well, delivering over 72% of the data packets regardless of the mobility rate at pause time '0's, whereas at high pause times with lower mobility it delivers over 68% of the data packets, compared with SEAD delivering between 73% and 69% of the packets and DSDV delivering between 17% and 65% of the packets. So that SEAD packet delivery ratio is independent of offered traffic load, with both protocols delivering between 73% and 69% of the packets. The AWDV and SEAD routing protocol perform better than the table-driven DSDV protocol. The DSDV delivers 20% of the data packets regardless of the mobility rate at pause time 0s, while at high pause times with lower mobility it delivers over 70% of the data packets, but DSDV proximity loses about 40%

more packets than AWDV and SEAD at higher mobility of pause times start from '0's to '40's. Nearly all of the dropped packets are lost because a stale routing table entry directed them to be forwarded over a broken link.

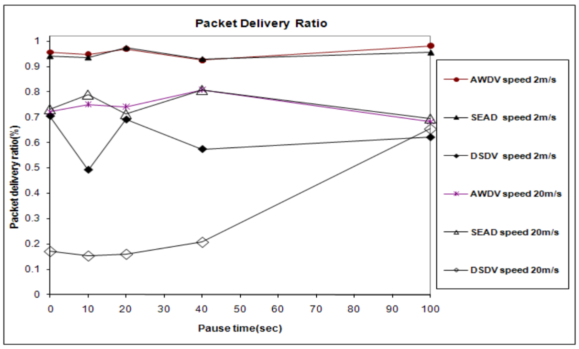


Fig.5(a) Packet delivery ratio at simulation time 100s.

b)- Simulation time 900s: At the lower movement speed of 2m/s, the AWDV routing protocol performed particularly well, delivering over 98% of the data packets regardless of mobility rate as shown in Fig.5(b) with the lower movement speed of 2m/s. So for AWDV, packet delivery ratio is independent of offered traffic load, delivering between 97% and 98% of the packets at SIMT 100s, compared with SEAD delivering between 97% and 98% of the packets and DSDV delivering between 87% and 96% of the packets. The AWDV and SEAD routing protocol perform better than the table-driven DSDV routing protocol. Whereas the DSDV loses about 11% more packets than AWDV and DSDV loses about 9% more packets than SEAD at lower 300s pause times (higher mobility). Nearly all of the dropped packets are lost because a stale routing table entry directed them to be forwarded over a broken link. At the higher movement speed of 20m/s as shown in Fig.5(b), the AWDV routing protocol performed particularly well, delivering over 80% of the data packets regardless of the mobility rate at pause time '0's and delivering over 99% of the data packets regardless of the mobility rate at pause time '900's. The SEAD routing protocol 81% of the data packets regardless of the mobility rate from pause time 0s to 50s, where very similar for AWDV and DSDV routing protocol at pause time 900s are delivering over 99% of the data packets. However, in all cases AWDV and SEAD proximity delivers over 88% of the data, and DSDV delivers over 65% of the data. But AWDV and SEAD are proximity very similar at pause times 100s to 900s, so that AWDV and SEAD routing protocol perform better than the table-driven DSDV protocol. But DSDV proximity loses about 14% more packets than AWDV and SEAD at higher mobility of pause times start from '0's to '100's and proximity loses about 3% at higher mobility of pause times start from '300's to '600's. Nearly all of the dropped packets are lost because a stale routing table entry directed them to be forwarded over a broken link.

It is obvious that from the above packet delivery ratio or called fraction at simulation time 100s and 900s the performance analysis of proposed AWDV protocol consistently outperforms than SEAD and DSDV routing protocol at movement speed 2m/s and 20m/s is similar with SEAD secure routing protocol. But the DSDV routing protocol has worst performance compared to both, where the DSDV is having worst performance for high mobility 20m/s, because it is not as adaptive to the route changes that occur.

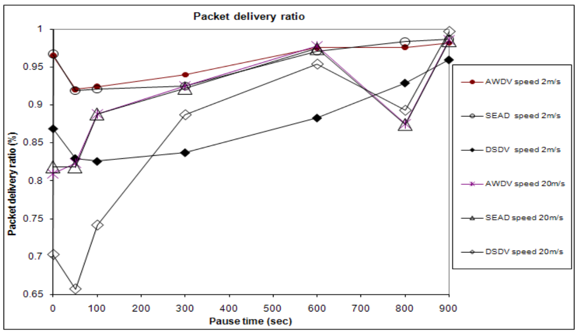


Fig.5(b) Packet delivery simulation time 900s.

5.3.2. Average end to end delays comparison

a)- Simulation time 100s: The average end-to-end delay of packet delivery at the lower movement speed of 2m/s is higher in AWDV and SEAD routing protocol as compared to DSDV in all cases as shown in Fig.6(a). But AWDV and SEAD are proximity the same level at pause time started from '0's to '20's, whereas the AWDV routing protocol is higher than SEAD from greater than '20's pause time. The average end-to-end delay of packet delivery at the higher movement speed of 20m/s the proposed AWDV secure routing protocol is good performance with lower delay packets delivery at pause time start in range '0's < pause time <'40's are compared with SEAD secure routing protocol and DADV routing protocol, where DSDV is higher and from pause time 40s to 100s at the end of simulation time are similar average end-to-end delay of both secure routing protocols, where DSDV is lower. So that in the higher movement speed of 20m/s the proposed AWDV and SEAD protocols dose not stable of routing protocol within environment of attacker and lost because a stale routing table entry directed them to be forwarded over a broken link with high movement speed.

b)- Simulation time 900s: The average end-to-end delay of packet delivery at the lower movement speed of 2m/s the proposed AWDV secure routing protocol is higher delay of packet delivery at pause time start in range '300's<pause time<'800's are compared with SEAD secure routing protocol and with DADV routing protocol at pause time from '500's to '900's as shown in Fig.6(b). The average end-to-end delay of packet delivery at the higher movement speed of 20m/s as the same the proposed AWDV secure routing protocol is higher delay of packet delivery at pause time started from '0's to '400's and from '700's to '900's compared with SEAD secure routing protocol, otherwise the proposed AWDV secure routing protocol is lower delay of packet delivery at in all cases of pause time.

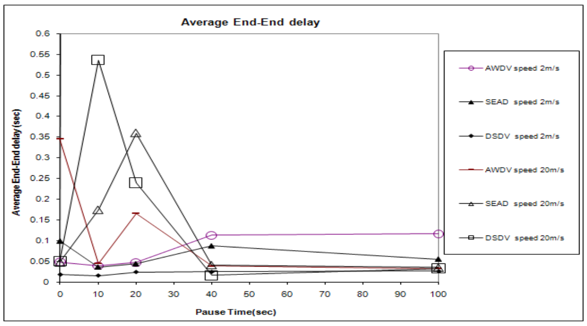


Fig.6(a) Average end to end delay at simulation time 100s.

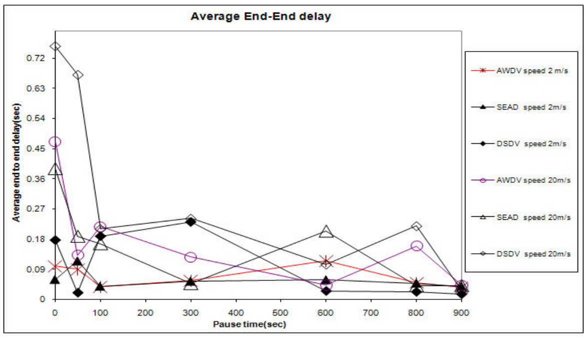


Fig.6(b) Average end to end delay at simulation time 900s.

It is obvious that the performance of AWDV under average end-to-end delay of packet delivery metric the authenticated digital watermarking algorithm consuming lower prepared delay of packet delivery than compared with the SEAD routing protocol using one way hash function with high consuming faster algorithm and the DSDV routing protocol has worst performance compared to both.

5.3.3. Normalized routing load comparison

a)- Simulation time 100s: In all cases, at the lower movement speed of 2m/s, DSDV demonstrates significantly lower normalized routing load than proposed AWDV and SEAD of secure routing protocol as shown in Fig.7(a). Moreover at the higher movement speed of 20m/s, the proposed AWDV and SEAD of secure routing protocol demonstrates significantly lower routing load than DSDV at pause time started from '55's to '100's end of simulation time.

b)- Simulation time 900s: The normalized routing load at the lower movement speed of 2m/s, the DSDV routing protocol is lower normalized routing load with compared the proposed AWDV and SEAD secure routing protocol as shown in Fig.7(b). The normalized routing load was higher in the proposed AWDV secure routing protocol with compared to DSDV routing protocol and SEAD secure routing protocol.

The normalized routing load at higher movement speed of 20m/s, the proposed AWDV and SEAD secure routing protocols are higher routing load than DSDV routing protocol as shown in Fig.7(b). Where the proposed AWDV and SEAD secure routing protocols are the same normalized routing load.

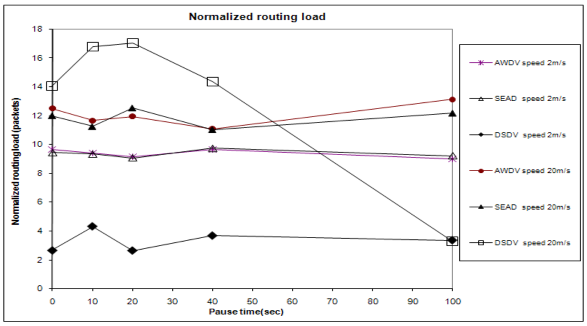


Fig.7(a) Normalized routing load at simulation time 100s.

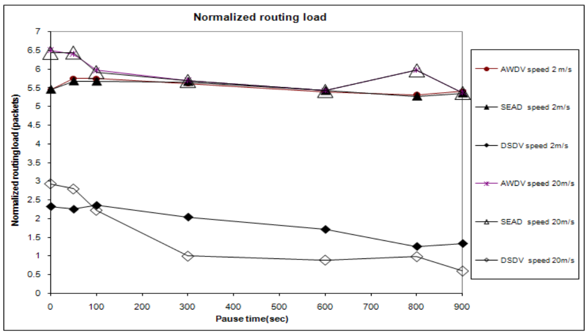


Fig.7(b) Normalized routing load at simulation time 900s.

5.3.4. Routing overhead comparison

a)- Simulation time 100s: The routing overhead as shown in Fig.8(a) is the number of routing overhead packets generated by routing protocols to achieve this level of data packet delivery. In all cases, at the movement speed of 2m/s and 20m/s, DSDV demonstrates significantly lower routing overhead. Moreover, the proposed AWDV secure routing protocol is demonstrates significantly higher routing overhead than SEAD secure routing protocol and DSDV protocol.

b)- Simulation time 900s: The routing overhead of the DSDV routing protocol is lower routing overhead than proposed AWDV and SEAD protocols as shown in Fig.8(b). The routing overhead was higher in the same level of the proposed AWDV and SEAD protocols.

It is obvious that from the routing overhead the performance analysis of proposed AWDV and SEAD are higher network bandwidth overhead than DSDV protocol, because it is required periodic authenticated route updates to inform other nodes to achieve a consistent routing table depending on malicious node and mobility, but the proposed AWDV protocol is higher because the authentic routing update generated by employ smaller incremental packet update one by one until completed the entry table periodically.

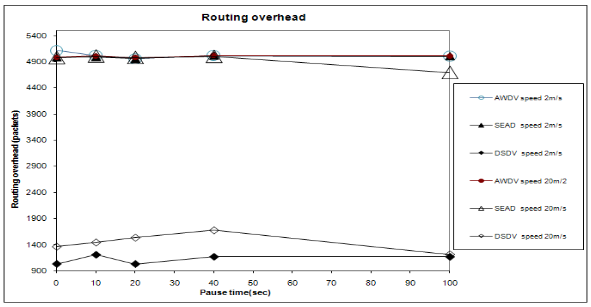


Fig.8(a) Routing overhead at movement simulation time 100s.

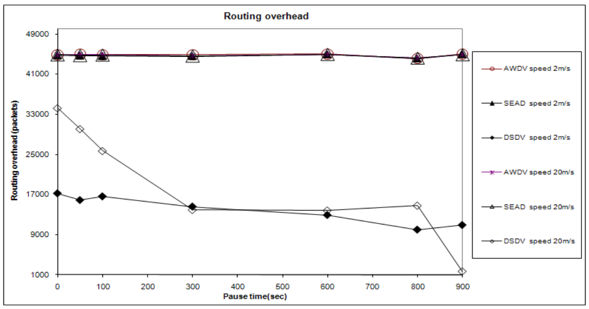


Fig.8(b) Routing overhead at movement simulation time 900s.

5.3.5. Drop packets comparison:

a)- Simulation time 100s: The drop packets by malicious nodes from the total drop packets at the lower and higher movement speeds of 2m/s and 20m/s, the performance analysis of proposed AWDV protocol is a lower drop packet by malicious node than the SEAD and DSDV protocols as shown in Fig.9(a).

b)- Simulation time 900s: The drop packets by malicious nodes from the total drop packets at the lower and higher movement speeds, the DSDV routing protocol is higher. But at higher movement speed 20m/s, the SEAD protocol is lower drop packet by malicious node at pause time start from '0's to '50's and from '450's to '900's as shown in Fig.9(b).

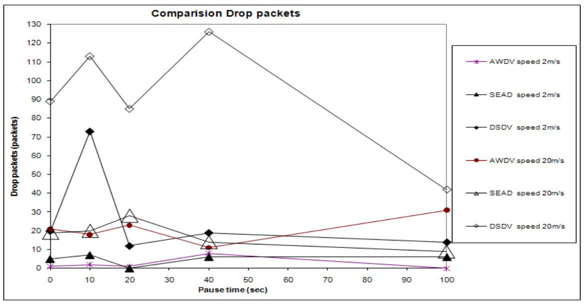


Fig.9(a) Drop packets at simulation time 100s.

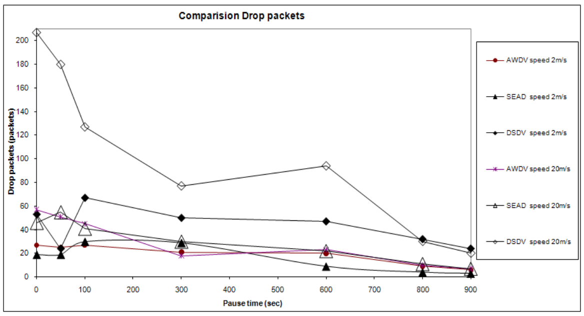


Fig.9(b) Drop packets at simulation time 900s.

6. Conclusion and Future Work

This paper proposed a novel authenticated digital watermarking algorithm in mobile ad-hoc distance vector routing protocol (AWDV) to provides a secure routing protocol and compared with two ad-hoc routing protocols such as SEAD secure routing protocol and traditional DSDV routing protocol. The performance analysis evaluation of simulation setup ns-2 and metrics are based on packet delivery ration, average end to end delay, normalized routing load, routing overhead and drop packets metrics. We have studied the results of the simulation models, which are showed the effect under various pause time and different movement mobility.

In this paper, over all we are suggesting that the proposed AWDV outscores the traditional DSDV and SEAD protocols in all aspects, and the proposed AWDV enhanced table-driven routing protocol DSDV provides the solution for the possible packet dropping attack in MANET. Moreover the performance of AWDV under average end-to-end delay of packet delivery metric the authenticated digital watermarking algorithm consuming lower fast prepared delay of packet delivery than compared with of the SEAD using one way hash function with high consuming faster algorithm and the DSDV routing protocol has worst performance compared to both, where it is having worst performance for high mobility 20m/s, because it is not as adaptive to the route changes that occur. In the future, extensive complex simulations could be carried out using this paper code, in order to gain a more in-depth performance analysis of the ad-hoc routing protocols with the source-initiated on-demand routing protocols.

References

[1] A. hashad and M. Gannan,"Performance evaluation of routing protocols for mobile ad hoc network ", ICCTD Inter. Conf. on Comp. Techno. and Development, IEEE Comp. Society, 13-15, Nov.2009.

[2] F. Bertocchi, P. Bergamo, G. Mazzini and M. Zorzi "Performance Comparison of Routing Protocols for Ad-Hoc Networks", IEEE GlobeCom 2003, San Francisco, California, USA, p.1033-1037, Dec 1-5, 2003.

[3] M. B. Aliwa, M. Hashem, M. T.EL-Sonni,"Performance Evaluation Routing Algorithm Protocols of Ad-Hoc Sensor Mobile Networks Using Ns-2 simulator", Pro of the First Inter Conf. on Info. Sys. & Techno. MES College of Eng, Kuttippuram, Kerala, india, Pp.1-16, Dec 14-15, 2007.

[4] N. Garg and R.P.Mahapatra,"MANET Security Issues", International Journal of Computer Science and Network Security, Vol.9, No.8, p.241-246, Aug.2010.

[5] G. Fang, L.Yuan, Z. Qingshun and Li Chunli,"Simulation and Analysis for the Performance of the Mobile Ad Hoc Network Routing Protocols", IEEE the Eighth Inter Conf on Elect Measurement and Instruments, vol.2, p.571-575, 2007.

[6] Ramesh B. and D.Manjula,"Performance Analysis of Mobile Ad Hoc Routing Protocols for Streaming Multimedia", Pro of the First Inter Conf on Info Systems and Tech MES College of Eng, Kuttippuram, Kerala, india, Pp.49-54, Dec 14-15, 2007.

[7] P. M. Jawandhiya, M. M. Ghonge, M.S.Ali and J.S. Deshpande," A Survey of Mobile Ad Hoc Network Attacks", Inter. Journal of Eng. Sci. and Technology, Vol.2, No.9, P.4063-4071, 2010.

[8] C. E.Perkins and P.Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers", In Proc. of the ACM SIGCOMM Conf. on Comm. Archit., Protocols, and Applications, P.234–244, August 1994.

[9] X. Hong, Kaixin Xu, and M.Gerla,"Scalable routing protocols for mobile Ad-hoc networks", University of California at Los Angeles IEEE Network, p.11-21, August 2002.

[10] N. Bhalaji, S.banerjee and A.Shanmugam," A Novel Routing Technique against Packet Dropping Attack in Ad-hoc Networks", Journal of Computer Science vol.4, No.7, p.538-544, 2008.

[11] Hi Deng, Wei Li and D. P. Agrawal," Routing Security in Wireless Ad Hoc Networks", IEEE Telecommunications Network Security Magazine, P.70-75, Oct.2002.

[12] A. Bansall and S. S.Bhadouria "Network Security and Confidentiality with Digital Watermarking", 2007 Inaugural IEEE International Conference on Digital Ecosystems and Technologies, p.325-328, 2007

[13] Y. Yusof and O. Khalifa, Member, IEEE,"Digital Watermarking For Digital Images Using Wavelet Transform", Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, Penang, Malaysia, p.665 – 669, 14-17 May 2007.

[14] Stefan Katzenbeisser and Fabien. Petitcolas, “Information hiding Techniques for Steganography and Digital watermarking", Copyright.2000 Artech house, inc

[15] J. Cox, Matthew L. Miller, and Jeffrey A. Bloom "Digital Watermarking Morgan Kaufmann Series in Multimedia Information and Systems", pub:Elsevier, San Francisco, by.Academic.Press,UnitedStatesof America, 2002.

[16] M.Mondal and D.Barik,"Spatial Domain Robust Watermarking Scheme for Color Image", 2010 IEEE-International Conference on Software and Computing Technology, vol,1, p.384-387, 2010.

[17] A.H. Shabaan, H. ElZouka and M. Abou ElNasr,″ Intrusion Detection System in wireless Ad-hoc Networks Based on Mobile Agent Technology", IEEE2010 2nd International Conference Computer Engineering and Technology, Chengdu, Vol.1, p.470-474,16-18 Ap.2010.

[18] Y. Hu, D.Johnson, and A. Perrig,"SEAD:Secure Efficient Distance Vector Routing for Mobile Wireless Ad-hoc Networks", In Proc. of the 4th IEEE Workshop on Mobile Comp. Syst. and Applications, 2002.

[19] Data and computer communications, fifth Edition, by William Stallings, page.297-300, 1997.

[20] L. Buttyan and J-P. Hubaux," Report on a Working Session on Security in Wireless Ad Hoc Networks", ACM SIGMOBILE Mobile Comp. & Comm. Review, New York, NY, USA, Vol.7, Issue.1, p.74-94, Jan.2003 .

[21] M. B. Aliwa, T. El-A. El-Tobely, M. M. Fahmy, M. EL Said Nasr and M. H. Abd El-Aziz,"A New Novel Fidelity Digital Watermarking Adaptively Pixel based on Medial Pyramid of Embedding Error in Spatial Domain and Robust", IEEE.2010-Inter. Conf. on Soft. and Comp. Techno.(ICSCT), Vol.1, p.19-26, 17-19, Oct. 2010.

[22] M. B. Aliwa, T. El-A. El-Tobely, M. M. Fahmy, M. EL Said Nasr and M. H. Abd El-Aziz,"A New Novel Fidelity Digital Watermarking Based on Adaptively Pixel-Most-Significant-Bit-6 in Spatial Domain Gray Scale Images and Robust", American Journal of Applied Sciences, Vol.7, No.7, pp.987-1022, Science Publication 2010.

[23] M. B. Aliwa, T. El-A. El-Tobely, M. M. Fahmy, M. EL Said Nasr and M. H. Abd El-Aziz,"Robust Digital Watermarking Based Falling-off-Boundary in Corners Board-MSB-6 Gray Scale Images", International Journal of Computer Science and Network Security (IJCSNS), Vol.9, No.8, p.227-240, August 30, 2009.

[24] Mobile Ad-hoc Networking, editor Stefano Basagni, Marco Conti, Silvia Giordano and Ivan Stojmenovic, by the Institute of Electrical and Electronics Engineers, Pub. in Canada, 2004, ISBN:0-471-37313-3.

[25] Mobile ad-hoc networks, from wireless LAN to 4G networks, editor George Aggelou, by the McGraw-Hill Companies, Inc. printed in USA, ISBN:0-07-141305-7, chapter.2, p.71,2005.

[26] The Ns-2 Manual, (formerly ns notes and documentation) The VINT project a collaboration between researchers at UC Berkeley, LBL, USC/ISI, and Xerox PARC, August 23-2006, p.160, generating traffic pattern files.

[27] Website: Tutorial for simulator ns-2, http://www.isi.edu/ nsnam/ns/tutorial/

[28] Website Running Ns & Nam Under Windows 9x/2000/XP cygwin, http://www.isi.edu/nsnam/ns/ns-cygwin.html.

[29] Website: Document lists various trace formats used by the NS-2 Network Simulator Ns-2, http://nsnam.isi.edu/ nsnam/index.php/NS-2_Trace_Formats.

[30] Website: Ns-2 Code for Random Trip Mobility Model, by S. Pal Chaudhuri, Rice University. http://monarch.cs. rice.edu/~santa/research/mobility/.

[31] J.-Y. Le Boudec and M. Vojnovic," Perfect Simulation and Stationarity of a Class of Mobility Models", IEEE Proceeding Annual Simulation Symposium Proceedings of the 38th annual Symposium on Simulation, IEEE Computer Society Washington, DC, USA, p. 72-79,2005.

[32] E. Altman, T. Jimenez, "Ns Simulator for beginners", Lectures note 2003-2004, univ.de Los Andes, Merida, Venezuela and ESSI, Sophia-Antipolis, France, pages.1-146, Dec.4-2003.

[33] E. M. Royer and C. K. Toh,"Areview of current routing protocols for mobile wireless networks", IEEE personal communications,Vol.6,No.2, p.46-55, Aprial 1999.

[34] D. B. Johnson, and D. A.Maltz,"dynamic source routing protocol for mobile ad hoc networks", Mobile Computing, edited by Tomasz Imielinski and Hank Korth, Kluwer Academic Pub.1996.

Mehemed Bashir Aliwa received the B.Sc. Degree in Computer Engineering on September 1, 1992 from the Engineering Academy, Tajoura-Libya and the M.Sc. Degree in Computer Engineering on March.2008 from the Arab Academy for Science, Technology and Maritime Transport College of Engineering and Technology, Alexandria-Egypt. He is currently pursuing the Ph.D. degree at the Electrical Engineering (Computer and Control Engineering) of the Faculty of Engineering TANTA University, Egypt. From 1992 to 1996 his was working in the research center of military industrialization, from 1996 to 1997 as a Lecturer at the School of Electronic Support and from 1997 to 2005 as a director, office of the global information network and the office of training and maintenance in computer system in Authority operations and training Libyan armed forces and he is promoted to brigadier engineer from 2011. His research interests include digital watermarking, hiding information, and routing protocol in mobile ad-hoc networks.