Secure Authentication Watermarking in Ad-hoc Destination-Sequenced Distance-Vector Routing Protocol

Mehemed Bashir Aliwa
EMAK International Academy an Oracle Academy, Cairo, Egypt.

Summary
Security is important in the routing protocol of mobile ad-hoc networks MANETs, it is necessary to protect against malicious attacks as well as in data transmission. The goal of mobile ad-hoc security is to safeguard the nodes' operation and ensure the availability of communication in spite of adversary nodes. The node operations can be divided into two phases, discover route path and forward data, both stages need to protect from attacks. In this paper, have been proposed SAWDV: Secure Authentication Watermarking in Ad-hoc Destination-Sequenced Distance-Vector routing protocol by improving a novel authenticated digital watermarking in mobile ad-hoc routing protocol AWDV based on the design of the Destination-Sequenced Distance-Vector DSDV. In order to support use with nodes to guard against wormhole and modification attacks. The result of the SAWDV was compared with the SEAD: secure efficient ad-hoc distance vector, AWDV and standard DSDV routing protocols, under the performance analysis of simulation using simulator ns-2 with security analysis. The results obtained prove that the SAWDV outscores the AWDV, SEAD and DSDV in all aspects. The SAWDV improve and enhance the security of AWDV provides the security solution for the possible packet dropping by wormhole and modification attacks in MANETs.

Key words:
Mobile ad-hoc network, attacks, secure routing protocol, digital watermarking, ns-2 simulator and metrics.

1. Introduction

Mobile ad-hoc network is defined as a network without infrastructure, meaning a network without the usual outing infrastructure like fixed routers and routing backbones[1][2]. MANET security is a new area for research that it has been faced many difficulties to implement. These difficulties are due to the absence of central authentication server, the dynamically movement of the nodes (mobility), for example the deployment of vehicular communication systems is strongly dependent on their security, and limited capacity of the wireless medium and the various types of vulnerability attacks[3]. These entire factors combine to make mobile ad-hoc a great challenge to the researcher[1]. Moreover, in fourth-generation wireless networks may require an integration of mobile ad-hoc network into external network to enhance the flexibility of the communication and roaming. This phenomenon is well-suited for commercial and military applications which yield additional benefit of roaming. However, integration of MANET with external network poses a serious security challenge for communication because of open and distributed nature of the ad-hoc network[4]. Mobile ad-hoc network has been used in different applications networks range[2] from military operations and emergency disaster relief to community networking and interaction among meeting attendees or students during a lecture[1]. This environment of different applications creates a provision for misbehaving nodes to induce active or passive attacks in the network in order to exploit the covert missions[4], for example of misbehaving nodes as wormhole attack, two nodes cooperate to construct a tunnel between them. This tunnel is built either by using wire cable, wireless transmission or any media[1], or modification attacks, misbehaving nodes can easily modifying routing information 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 information[5], because it is sensitive characteristics in mobile ad-hoc network of dynamic topologies, bandwidth constrain, energy-constrained, all of these cause limited physical security[4][6]. There are a number of mechanisms that have been proposed in the past[2][7][8][9], for instance, but those protocols are compromised in many ways. So, there is a need of a technique to provide privacy and security for the mobile nodes while communicating between ad-hoc networks to fixed network and vice versa, so some of secure routing protocols using cryptography as SEAD routing protocol[8] and other using watermarking as AWDV routing protocol[7].

Cryptography and watermarking[10] both tackle the issue of computer security, but watermarking have additional uses other than securing applications. For multimedia and network security such as wireless MANETs issues are typically handled through cryptography; however, cryptography only ensures confidentiality and authenticity[10], when a message is transmitted through a public channel such as an open network or wireless node in MANETs, but it can be detected by malicious attacks, which can observe or intercept a transmission channel. Because there is a change in the structure of the data (scrambled and

Manuscript received May 5, 2014
Manuscript revised May 20, 2014

unreadable[10]) it can arouse suspicion and curiosity. Moreover, digital watermarking differs from cryptography, because it leaves the original medium or data almost entirely unaltered, thus it is an effective way to protect secure data to multimedia data even after its transmission[7], then, digital watermarking solutions can be used to prevent the impact of active or passive attacks and which provide evidence of its authenticity[10].

The organization of the rest paper is as follows: In section.2, the related works of routing protocol. In section.3, the proposed secure authentication digital watermarking in MANETs. In section.4, methodology described simulation model and performance metrics. In section.5, evaluation results using ns-2 simulator, finally, security analysis of routing protocols and conclusion.

2. Related Works in MANETs

The ad-hoc routing protocols have been studied extensively as the following:

A. AWDV

Authenticated digital watermarking in mobile ad-hoc distance vector routing protocol (AWDV)[7]. It is used to embed watermark in each authentic route advertisements/update to create authentic "watermarked packet" entry in a routing update. First: Each node in the topology network create randomly a numerical value matrix of '128' bytes in size (a, b) at each authentic route update. Second: Each node store a public watermark $W\in\{0, 1\}^{\rho}$. Secret key (ρ) is the length of bits, as input is used at encoder process to produce authentic route update of 'watermarked packet'. Third: Encoder: Step.1: Extract value $P_{(i,j)}$ from created randomly a numerical matrix and converted into the binary bits, then set of the most significant bit (MSB_6) in each value $P_{(i,j)}$ within the boundary board of corner BBC, 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 EMB, thus the value $P_{(i,j)}$ can be further segmented into eight intervals is described in[11]. Step.2: Pseudo encoder code of adaptively value $P_{(i,j)}$ adjustment process by applying in falling-off-boundary in corners board set of MSB ($APAP\text{-}FOBCB_{MSB6}$)in[11][12] of the created randomly numerical value matrix. Let's have a binary watermark $W_{(\rho)}$, where the bits EMB={EMB_0, EMB_1,…, $EMB_{(k)}$}, and set MSB_n in each value $P_{(i,j)}$ of BBC, whereas n=6 in the range of $5< n \leq 8$ and k = 0, 1, 2,..., ρ – 1, read pseudo encoder code in $FOBCB_{MSB6}$[11], then we will applied pseudo encoder code under the FOBCB algorithm of the numerical value matrix[12]. The $APAP\text{-}FOBCB_{MSB6}$ scheme[11] using to embed watermark in a BBC, and before embedding requires a checking between the MSB_6 in the BBC of matrix value $P_{(i,j)}$ within the EMB, to inform the "forward authentic watermarked packet value". Step.4: Decoder, the node advertises by broadcasts routing information using the mechanism of message authentication 'watermarked packet', then the receiver (node), received authentic route update with "watermarked packet to neighbors node, each node required route selection (select route with higher destination sequence number, or select the route with better metric when sequence numbers are equal), then applying procedure of comparator between extracted watermark and public watermark to provides the successfully of the mechanism authentication as following: First: Extracted watermark from the FOBCB of the received 'watermarked packet' simultaneously by using inverse the same procedure of embedding algorithm, then the watermark in original form is thus obtained. Second: After successfully extracted watermark required to comparator between the extracted watermark and public watermark to indicated in entire table of authentic route $AWDV\in\{0,1,\infty\}$, if '0' indicate broken link, '1' authentic route and '∞' it is not authenticated [7].

B. SEAD

SEAD secure routing protocol[8] is a part of the DSDV. The SEAD use efficient one-way hash functions. It is built on a one-way hash function "H", it maps an input of any length to a fixed-length bit string. Thus, $H:\{0,1\}^*\rightarrow\{0,1\}^{\rho}$, where ρ is the length in bits of the hash output. To create a H, a node chooses a random $x\in\{0,1\}^{\rho}$ and computes the list of values: h_0, h_1, h_2, h_3,…, h_n, where $h_0=x$, and $h_i=H(h_{i-1})$ for $0 < i \leq n$, for some *n*. The node at initialization generates the elements of its hash chain, from "left to right", or "right to left" in order of increasing, or decreasing subscript *i*, and it is element to secure its routing updates. Each node have public-key, it is used to sign a new hash chain element for itself. We assume that an upper bound can be placed on the diameter of the ad-hoc network, let us consider '*m*' is the number of nodes, so that the upper bound for the hop counts is < (m-1). The method used 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 is 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 calculated using H be h_0, h_1, h_2, h_3,…, h_n, where *n* is divisible by *m*, then for a sequence number 'I' in some routing update entry, let k = ((n/m)–I). The group of elements used for routing update with sequence number 'I' and distance *j* as: h_{km}, h_{km+1},…,h_{km+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 h_{km+j} here is used to authenticate route update entry for that sequence number 'I' and

distance *j*, where 0< I ≤ (m-1) and n=(m-1)×m. So nodes receiving any routing update can easily authenticate [7].

C. *DSDV*

The DSDV routing protocol[9] based on the classical bellman-ford routing mechanism. 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[2]. 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, called an "incremental". First the full dump. This type of packet carries all available routing information. 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, 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 [13][14].

3. Proposed Secure Authentication Watermarking in Ad-Hoc MANET's

In this section, have been proposed secure authentication watermarking in ad-hoc destination sequenced distance vector routing protocol SAWDV by modifying AWDV: Authenticated digital watermarking in ad-hoc distance vector routing protocol[7]. It is used to embed a watermark as an authentication and hide the (owner address of source node as a tamper evidence/detection and number of hops to reach the destination node), in order to create authentic "watermarked packet" entry at each authentic route update, whereas the mobile nodes maintain an additional table with a new table entry of authenticated route. The table entries are used to store routing information by the incremental authentic route information packet. New authentic route broadcast contain the address of the destination, sequence number of the information received regarding the destination, and "watermarked packet". The following section outlines the mechanism of authenticated digital watermarking.

3.1. Encoder Mechanism of Routing Authentication

First: Each node in the topology network creates a cover gray scale image, which only gets the coordinates and pixels as a matrix of gray scale values as shown in Fig.1 of size (M, N) with the '128' byte at each authenticated routing update. Notice that the value $P_{(i,j)}$ is the corresponding '8' bit pair value of gray scale in the range of $0 \leq P_{(i,j)} < 2^8$. **Second:** Each node store the binary watermark(*W*) shown in Fig.1 as a data authentication, $W \in \{0, 1\}^{\sigma}$ where (σ) is the length of watermark bits, it used at encoder process to produce authentic route advertisement of 'watermarked packet'. Also, it used to match between the extracted watermark and original watermark, to provide the successful authentication routing function at each route advertisement/update. **Third:** The mechanism (encoder) is used for each node to distribute authentic "watermarked packet" at each route advertisement. It will use the embedding process of an adaptive value $P_{(i,j)}$ adjustment process, by applying in the falling-off-boundary in board corners using the MSB called ($APAP\text{-}FOBCB_{MSB6}$)[11][12] as following steps:

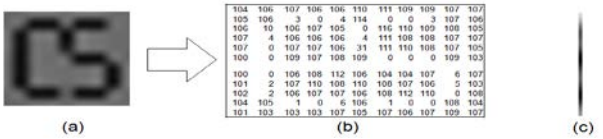

Fig.1: (a) Cover Gray Scale Image of Size (11,11). (b) Coordinates of Gray Scale Value (11,11). (c) Binary Watermark of Size (1,8)

Step 1: *First*, value $P_{(i,j)}$ is extracted from the created gray scale image and converted into the binary bits as ($LSB_{(1,2,3,4)}$ and $MSB_{(5,6,7,8)}$). *Second*, in each value $P_{(i,j)}$ within the BBC set MSB_6, when the MSB_6 of the value $P_{(i,j)}$={the embedded (watermark bits *W*, owner source Ethernet address (Ms) and number of hop to reach the destination node (Hd)) these are called ($WMsHd_{(\beta)}$)}, then do nothing, where β is the length of the embedding bits. Otherwise when the MSB_6 in the created value $P_{(i,j)}$ is not equal the embedded bits, it means that the $MSB_6 \neq WMsHd_{(\beta)}$, thus the value $P_{(i,j)}$ can be further segmented into eight intervals in [11]. **Step 2:** The pseudo encoder code of $APAP\text{-}MSB_n$ set of the MSB_6 of the created gray scale image. Let us have the maximum number of nodes in the topology (network diameter) = 50, then the owner source Ethernet address (Ms) of sender $node_(0)→ $node_(49) required 6-bits and the number of hops to reach the destination node (Hd) receiver required 6-bits and the binary watermark of size (1,8) required 8-bits. Thus the $WMsHd_{(\beta)}$ are converted to the vector bits equal [EMB={EMB_0, EMB_1,…, $EMB_{(k)}$}]. The MSB_n in each value $P_{(i,j)}$ of the boundary are used in the board corners of the

created cover. Then $WMsHd_{(\beta)}$ can be embedded in the BBC of the created cover in first round 5 byte=40 bit, for more robust in second round 4byte=32bit, whereas n=6 in the range of $5<n\leq 8$ and k = 0, 1, 2, 3,..., β – 1 and β is the length of embedding vector bits=20 bits: k= 0;

for *i* = 0 to M - 1
for *j* = 0 to N - 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 & EMB_k = 1), then
if ($P_{(i,j)} \geq 0$ & $P_{(i,j)}$ <2^n-1),then "$P_{(i,j)}$=2^n-1;
else if ($P_{(i,j)} \geq 2^n$ & $P_{(i,j)}$<3×2^n-1), then
if ($P_{(i,j)} \geq 2^n$ & $P_{(i,j)}$<5×2^n-2), then
"$P_{(i,j)}$ = (2^n) -1; else "$P_{(i,j)}$ = 3×2^n-1; end;
else if($P_{(i,j)} \geq 2^n+1$ & $P_{(i,j)}$<5×2^n-1), then
if($P_{(i,j)} \geq 2^n+1$ & $P_{(i,j)}$<9×2^n-2), then
"$P_{(i,j)}$=(2^n+1)-1; else "$P_{(i,j)}$=5×2^n-1; end;
else if($P_{(i,j)} \geq 3\times 2^n$ & $P_{(i,j)}$<7×2^n-1), then
if($P_{(i,j)} \geq 3^n$ & $P_{(i,j)}$<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 ($P_{(i,j)} \geq 2^n-1$ & $P_{(i,j)}$ <2^n), then
if ($P_{(i,j)} \geq 2^n-1$ & $P_{(i,j)}$ <3×2^n),then
"$P_{(i,j)}$=(2^n-1)-1; else "$P_{(i,j)}$ = 2^n; end;
else if ($P_{(i,j)} \geq 3\times 2^n-1$ & $P_{(i,j)}$<2^n+1), then
if ($P_{(i,j)} \geq 3\times 2^n-1$ & $P_{(i,j)}$<7×2^n-2), then
"$P_{(i,j)}$=(3×2^n-1)-1; else "$P_{(i,j)}$ =2^n+1; end;
else if ($P_{(i,j)} \geq 5\times 2^n-1$ & $P_{(i,j)}$<3×2^n), then
if ($P_{(i,j)} \geq 5\times 2^n-1$ & $P_{(i,j)}$<11×2^n-2), then
"$P_{(i,j)}$=(5×2^n-1)-1; else "$P_{(i,j)}$=3×2^n; end;
else if ($P_{(i,j)} \geq 7\times 2^n-1$ & $P_{(i,j)}$ <2^n+2), then
"$P_{(i,j)}$ = (7×2^n-1)-1; end; end;
end; end; end; end; end;
if (k < (*β* - 1)), then k = k + 1;else k = 0; end; end; end.

From pseudo encoder of APAP-FOBCB $_{MSB6}$ is applied to the cover image, to embed the $WMsHd_{(\beta)}$ bits in the BBC of the gray scale, and before embedding, it is require checking between the MSB_6 in the BBC of the created gray scale within the EMB of the embedding $WMsHd_{(\beta)}$ bits, depending on the nearest adaptive value, to inform the forward authentic watermarked packet value P" $_{(i,j)}$ obtained by a APAP-FOBCB$_{MSB6}$ scheme.

3.2. Decoder Mechanism of Routing Authentication

The node advertises by broadcasting route information using the mechanism of message authentication 'watermarked packet'. The destination node does not use an average weighted settling time in sending triggered updates, to prevent attacks from nodes that might maliciously not use the delay. The destination node is received an authentic route advertisement contain: (destination address, sequence number and watermarked packet) from a neighbor's node. Each node requires route selection, selecting a route with a higher destination sequence number to ensure using the newest information from the destination. It then applies a procedure of comparator process between matching watermark and public-watermark as an authentication. Its then matches between the owner address of source node received and that hidden in a watermarked packet, as tamper evidence/detection, to provide the successful authentication at each route advertisements/update as the following**:** First: The owner address of source node, watermark and the number of hops is gets from the FOBCB set of the MSB_6 of the received 'watermarked packet', that is extracted simultaneously by using the inverse of the same procedures for the embedding algorithm, depending on the sequence seed, to ascertain manipulation between the BBC. Then the owner address of source node, watermark bits, and the number of hops are thus obtained in original form. Second: Each node requires this comparator process in the topology network after successfully extracting the hidden information from the watermarked packet (owner address of source node, watermark and number of hops): (i). The owner address of the source node received is compared with routing information and with that hidden in watermarked packet received as a tamper evidence/detection. The goal is to prevent wormhole and modification attacks from nodes that might maliciously not use the record packets, or modification information routing at one location in the network, and to prevent impersonation, spoofing or replays in which the attacker sends old advertisements of routing information to a node causing it to update its routing table with stale routes. (ii). Extracted watermark is matched with original watermark as a data authentication process to provide integrity and availability. After the successful authentication of the updated routing information for the entire table with the hidden number of hops to reach the destination node, this is extracted from watermarked packet and indicated in the entirely new table of routing authentication SAWDV∈{0,1,∞} at each smaller incremental of authentic route update, to avoid spoofed routes or the formation of routing loops through malicious node or redirection from the shortest path by malicious action, whereas '0' indicates a broken link, '1' an authenticated link, and infinite '∞' an unauthenticated link, according to the install time for the entire table when an entry was made (used to delete stale entries route from table).

4. Methodology

4.1. Simulation Model and Setup

A detailed simulation model based on network simulation ns-2[15][16][17][18] is used in the evaluation and attempting to measure the performance analysis protocols on a particular performance under a range of five metrics. The standard ns-2 simulator distribution

runs on Linux. However, a package for running ns-2 on Cygwin Linux Emulation for windows is available[17]. An attempt was made to implement SAWDV in ns-2 simulator with environment of attacker and compared with three routing protocols (DSDV, SEAD and AWDV). The parameters used for our simulation are given in Table.1. The routing protocols are evaluated on the simulation of '50' wireless nodes forming an ad-hoc network, with varying movement patterns of mobility model used random waypoint model[19] and one file traffic model loads, using Constant Bit Rate (cbr) service is used for connections. So that, we chose a space in order to force the use of longer routes between nodes over a rectangular (1000m×1000m) flat space for different simulation time (SIMT) with movement patterns generated for '5' different pause times: 0, 10, 20, 40, and '100'seconds for SIM 100 s, and '7' different pause times: 0, 50, 100, 300, 600, 800 and '900's for SIMT '900's , a pause time of '0's corresponds to continuous motion, and a pause time of '100' (the length of the simulation) corresponds to end of stop motion at SIMT 100s and as the same of SIMT 900s, because the performance of the protocols is very sensitive to movement pattern. In order to enable direct, fair comparisons between the protocols, it was critical to challenge the protocols with identical loads and environment attacker. From running simulator ns-2, we are generated output trace files and animator files, for each routing protocol, whereas the output trace file formats[18] are most important file in our experiment, which are analysis the outputs to record the packets and compute the performance metrics graphs, and the output animator files can be visualized in network animator[16].

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

Parameter	Value
Number of nodes	50
Area size of the topography (x,y) meter	(1000, 1000) m
Traffic type	cbr
Node transmission range (Wireless range)	150 m
Number of traffic sources	10
Send rate of traffic	'1' pkt/sec
Mobility (Movement speed of node)	Lower speed 2m/sec Medium speed (5 and 10) m/sec Higher speed 20 m/sec
The mobility model used	Random waypoint model
Created gray scale image of size (a, b)	(11, 11)
The range of gray scale	0 ≤ value < 256
Embedding in most significant bit used	MSB_n, n = 6
Simulation run time (second)	'100's, '900's
Pause time (s) at simulation time 100sec	0, 10, 20, 40, 100 second
Pause time (s) at simulation time 900sec	0, 50, 100, 300, 600, 800, 900 second

4.2. Performance Metrics

Five important performance metrics are evaluated, which are quantitatively measured the performance and activities that are running in ns-2 simulation.

- Drop of Packets (DP): It is to determine the amount of packets that are dropped by malicious nodes from the total dropped packets[20].
- Routing Packet Overhead (RPO): It is the total number of transmissions routing packets[2][13][14].
- Average End-to-End Delay (AED): It is defined the all possible delays caused by buffering during route discovery, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times[2][13][14][21]:

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

- Normalized Routing Load (NRL): The number of routing packets transmitted per data packet delivered at the destination[2][6][13][14].

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

- Packet Delivery Fraction (PDF): it 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, which defined the ratio of the data packets delivered to the destinations to those generated by the CBR sources, so the higher value is better result[2][14][20][21]:

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

5. Evaluation Results Using ns-2 Simulator

This section reports the results of the secure authenticated digital watermarking in mobile ad-hoc networks, undergone through simulation compared with traditional DSDV, AWDV and SEAD routing protocols. The results are summarized by measuring the performance metrics.

5.1. Packet delivery comparison

First, at simulation run time 100 sec, it is simulated at a lower and higher movement speed of (2, 5, 10 and 20) m/sec, the proposed SAWDV and AWDV protocols performed particularly well, delivering over in between 95% to 99% of the data packets regardless of mobility rate as shown in Fig.2 and Fig.3. So for SAWDV, packet delivery ratio is independent of offered traffic load, delivering between 95% and 99% 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.

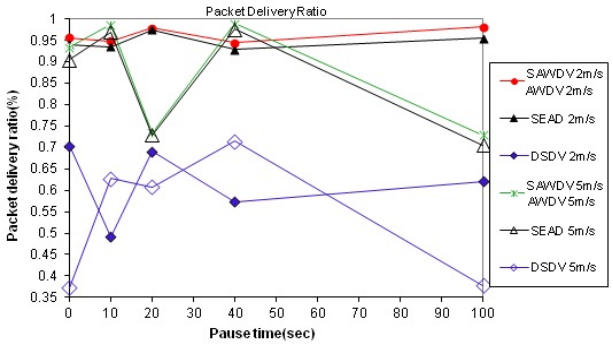

Fig.2: Packet Delivery Ratio at SIMT 100s with Mobility 2 & 5m/sec

The SAWDV routing protocol performs better than the table-driven DSDV and SEAD protocols. DSDV delivers over 70% of the data packets regardless of mobility rate as shown in Fig.2, with the lower movement speed (LMS) of (2m/sec). But DSDV loses about 46% more packets than SAWDV, AWDV and DSDV loses about 44% more packets than SEAD at lower pause time = 10s with higher mobility. At the higher movement speed of 20m/s seen in Fig.3, the proposed SAWDV and AWDV routing protocols performed particularly well, delivering over 73% of the data packets regardless of the mobility rate at pause time '0's. Conversely, 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. The SEAD packet delivery ratio is independent of traffic load offered and malicious node attacks, with both protocols delivering between 73% and 69% of the packets. The SAWDV, AWDV and SEAD protocols 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 higher pause time with LMS it delivers over 70% of the data packets. But DSDV proximity loses about 40% more packets than SAWDV, AWDV and SEAD at higher mobility speed (HMS) with pause times starting from '0's to '40's

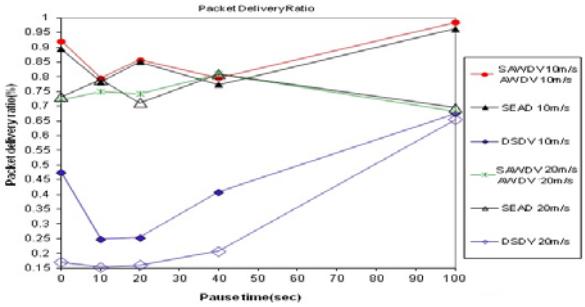

Fig.3: Packet Delivery Ratio at SIMT 100s with Mobility10 & 20m/sec

Second, at simulation run time 900 sec, it is simulated at a LMS of 2m/s, the proposed SAWDV and AWDV protocols performed particularly well, delivering over 99% of the data packets regardless of mobility rate as shown in Fig 4 with the LMS of 2m/s.

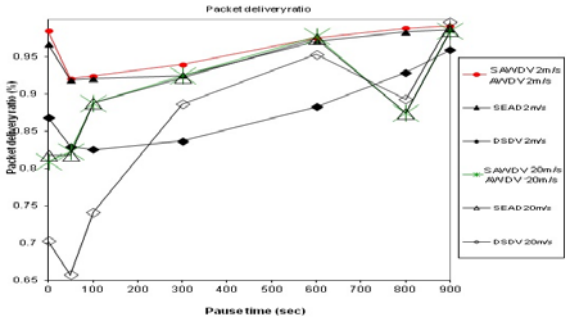

Fig.4: Packet Delivery Ratio SIMT 900s with Mobility 2 & 20m/sec

So for SAWDV, packet delivery ratio is independent of offered traffic load, delivering between 93% and 99% of the packets at SIMT 900s, compared with SEAD delivering between 92% and 97% of the packets and DSDV delivering between 85% and 96% of the packets. The SAWDV, AWDV and SEAD protocols perform better than the table-driven DSDV routing protocol, whereas the DSDV loses about 11% more packets than SAWDV and AWDV, but DSDV loses about 9% more packets than SEAD at lower pause time= 300s. At HMS of 20m/s as shown in Fig.4, the SAWDV protocol performed particularly well, delivering over 80% of the data packets at pause time= '0's and delivering over 99% of the data packets at pause time= '900's. While SEAD 81% of the data packets regardless of the mobility rate from pause time (0s to 50s), where very similar for SAWDV, AWDV and DSDV protocols at pause time 900s are delivering over 99% of the data packets. However, in all cases SAWDV, AWDV and SEAD proximity delivers over 88% of the data, and DSDV delivers over 65% of the data. But SAWDV, AWDV and SEAD are proximity very similar at pause times in range from 100s to 900s, so that SAWDV, AWDV and SEAD protocols perform better than the table-driven DSDV protocol. But DSDV proximity loses about 14% more packets than SAWDV and SEAD at HMS in pause time start from '0's to '100's and proximity loses about 3% at HMS in pause time start from '300's to '600's.

Third, so that from simulation run time (100s and 900s), it is obvious that from the packet delivery ratio, the performance analysis of the proposed SAWDV routing protocol is significantly higher outperforms than AWDV and SEAD routing protocols at movement speed 2, 5 and 10m/sec. But the DSDV protocol has worse performance than both others, whereas packet delivery ratio is independent of offered traffic load and malicious node attacks. DSDV has the worst performance for a HMS of 20m/s, because it is not as adaptive to the route changes that occur with HMS and routing table overflow by malicious node create routes to nonexistent nodes. Nearly all of the dropped packets are lost in DSDV because a malicious node attacks

selectively drop packet, and all of the dropped packets are lost in SAWDV, AWDV and SEAD at the pause time=20s by vertex cut of malicious nodes attack to the networks, as shown in Fig.2. Moreover, when topology of a network is dynamic, the routing protocols are unstable until update packets propagate throughout the network. Thus, to maintain connectivity, information needs to be periodically updated throughout the entire network. From the simulations of packet delivery ratio run, it is obvious that the performance is best when node mobility rates are lower. The proposed SAWDV enhanced AWDV and table-driven DSDV provides the best solution to the possibility of packet dropping attacks in mobile ad-hoc networks.

5.2. Average end to end delays comparison

First, at simulation run time 100 sec, it is simulated at a LMS and HMS of (2, 5, 10 and 20) m/sec, the average end-to-end delay of packet delivery in SAWDV, AWDV and SEAD routing protocols as compared to DSDV protocol in all cases is shown in Fig.5 and Fig.6. But SAWDV, AWDV and SEAD proximity are the same level at pause time from '0's to '20's. While SAWDV protocol is higher than SEAD at pause time greater than '20's. The average end-to-end delay of packet delivery at the HMS of 20m/s is dealt with well and with a lower packet delivery are delayed in SAWDV and AWDV routing protocols at pause time in range from ('0's < pause time <'40's), compared with SEAD and DSDV protocols is higher. From pause times in range from 40s to 100s at the end of SIMT, seen a similar average end-to-end delays occur in both secure routing protocols, whereas DSDV is lower. In the HMS of 20m/s, the proposed SAWDV, AWDV and SEAD protocols are not stable within the broken link occurred with HMS.

Second, at simulation run time 900 sec, the average end-to-end delay at the LMS of 2m/s is higher in the range of ('300's < pause time < '800's) of packet delivery with a routing protocols (SAWDV and AWDV), as compared with routing protocols (SEAD and DSDV) at pause time from '500's to '900's, as shown in Fig.7. But at the HMS of 20m/s it is the same delay of proposed SAWDV protocol with AWDV protocol, where 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 secure routing protocol SEAD. Otherwise, the proposed SAWDV routing protocol offers a lower delay of packet delivery for all pause times. Third, so that from simulation run time (100s and 900s), it is obvious that the performance of the proposed SAWDV routing protocol yields lower prepared delays under average end-to-end delay of packet delivery metric of the secure authenticated digital watermarking algorithm than compared with the SEAD routing protocol and with similar delay of AWDV routing protocol. But with the secure routing protocol SEAD use one way hash chains are consumed very fast execution algorithm, and the DSDV routing protocol has the worst performance compared to both, because a spoofed route or fabricated routing messages injected into the network or routing messages altered in transit.

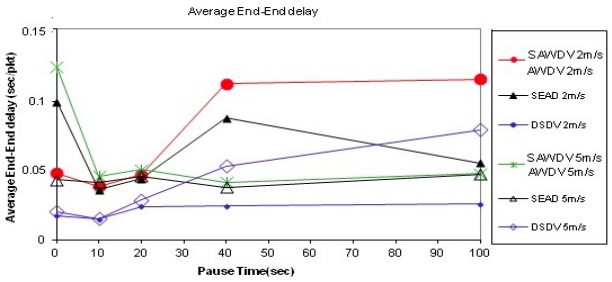

Fig.5: Average End to End Delay at SIMT 100s with 2 & 5m/sec

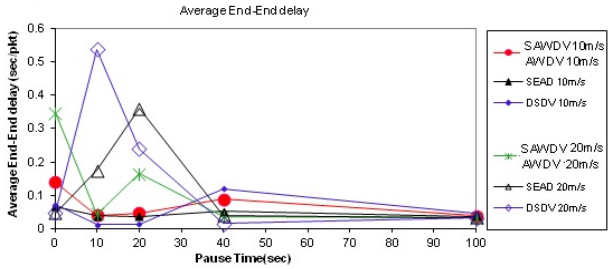

Fig.6: Average End to End Delay at SIMT 100s with 10 & 20m/sec

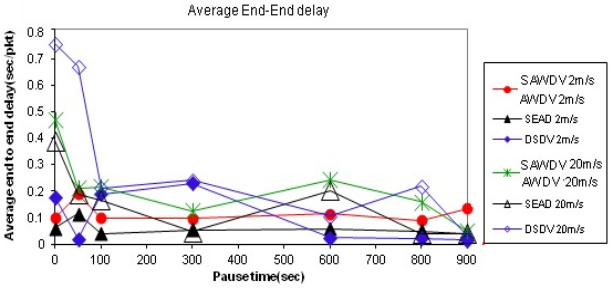

Fig.7: Average End to End Delay at SIMT 900s with 2 & 20m/sec

5.3. Normalized routing load comparison

First, In all cases, at simulation run time 100 sec, it is simulated at a LMS and HMS of (2, 5, 10 and 20) m/sec, the DSDV demonstrates significantly lower normalized routing load than SAWDV, AWDV and SEAD routing protocols as shown in Fig.8 and Fig.9. Moreover, at the HMS of 20m/s, the proposed SAWDV, AWDV and SEAD protocols demonstrates significantly lower routing load than DSDV at pause time started from '55's to '100's end of simulation time.

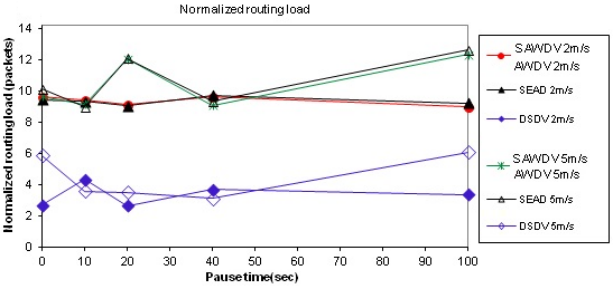

Fig.8: Normalized Routing Load at SIMT 100s with 2 & 5m/sec

Second, at simulation run time 900 sec, at LMS the normalized routing load of 2m/s, while DSDV is lower normalized routing load with compared the SAWDV, AWDV and SEAD routing protocols as shown in Fig.10. The normalized routing load was higher in the SAWDV AND AWDV protocols, when compared to DSDV and SEAD protocols. The normalized routing load at HMS of 20m/s, the SAWDV, AWDV and SEAD protocols can carry higher routing loads than DSDV, as shown in Fig.10. The SAWDV, AWDV and SEAD routing protocols yield the same normalized routing load.

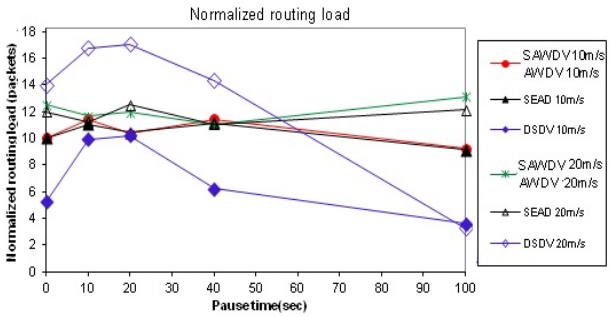

Fig. 9: Normalized Routing Load at SIMT 100s with 10 & 20m/sec

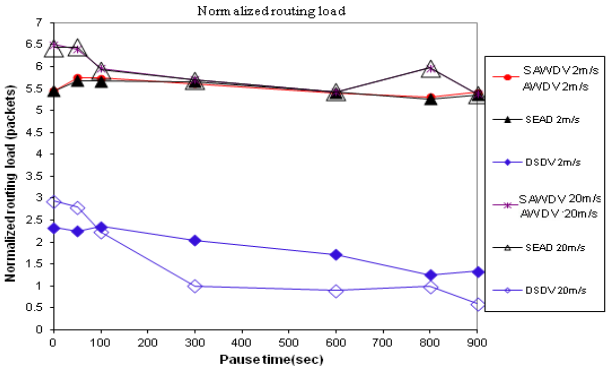

Fig.10: Normalized Routing Load at SIMT 900s with 2 & 20m/sec

5.4. Routing overhead comparison

In all cases, at simulation run time 100s and 900s, the performance analysis of routing overhead are shown in Fig.11, Fig.12, Fig.13, Fig.14 and Fig.15, the SAWDV, AWDV and SEAD routing protocols these are required higher network bandwidth overhead than traditional DSDV routing protocol, because they are required periodic authentic route updates to inform other nodes and to achieve a consistent routing table depending on the malicious action node attacks and mobility.

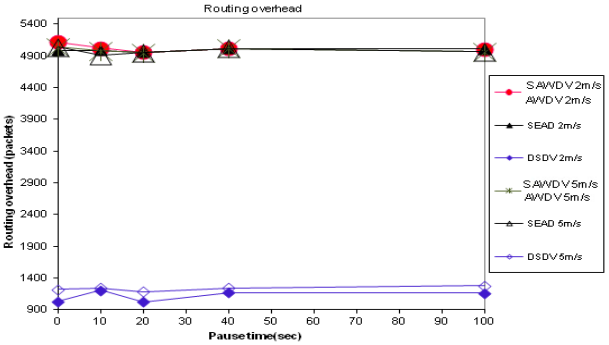

Fig.11: Routing Overhead at SIMT 100s with 2 & 5m/sec

The routing overhead in SAWDV protocol was higher than both other protocols, because the authentic routing update was generated by employing "smaller incremental" updates one by one (periodically) until the entry table was completed. The watermarking algorithm "consuming lower execution algorithm" prepared sum of delay of authentic routing update than compared with the one way hash chains are consumed very fast execution algorithm as shown in Fig.14 and Fig.15.

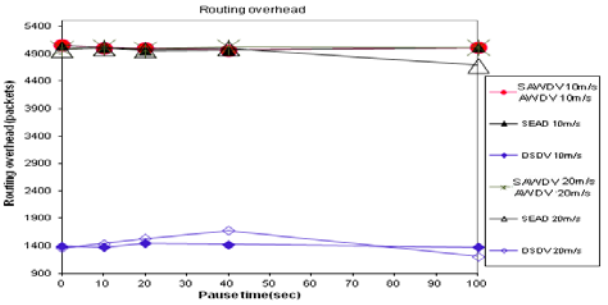

Fig.12: Routing Overhead at SIMT 100s with 10 & 20m/sec

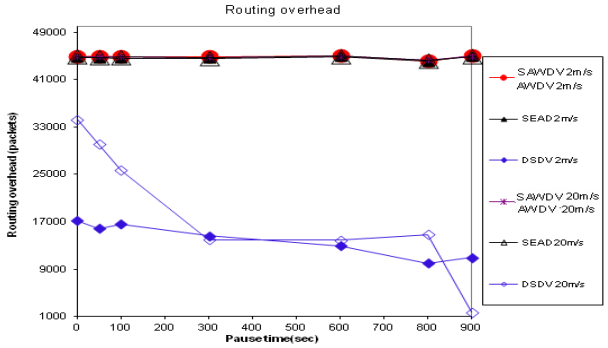

Fig.13: Routing Overhead at SIMT 900s with 2 & 20m/sec

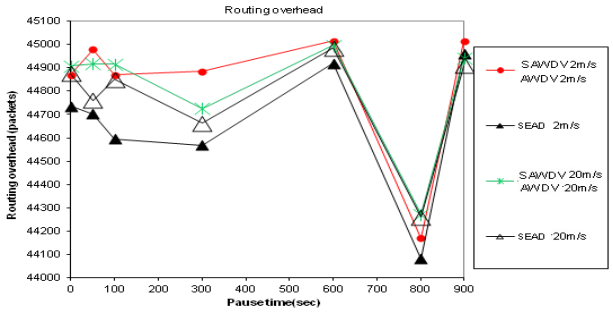

Fig.14: Routing Overhead at SIMT 900s with 2 & 20m/sec.

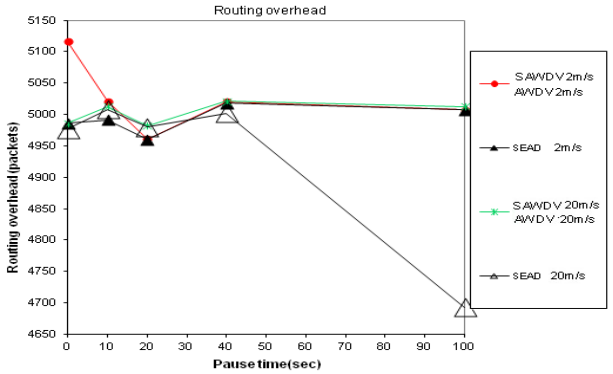

Fig.15: Routing Overhead of SAWDV and SEAD with 2 & 20m/sec

5.5. Drop packets comparison:

In all cases, the packet dropped at the LMS and HMS of (2, 5, 10 and 20) m/s, It is obvious that the SAWDV and AWDV routing protocols suggests a drop fewer packets due to malicious node attacks than the SEAD and DSDV protocols, as shown in Fig.16 and Fig.17.

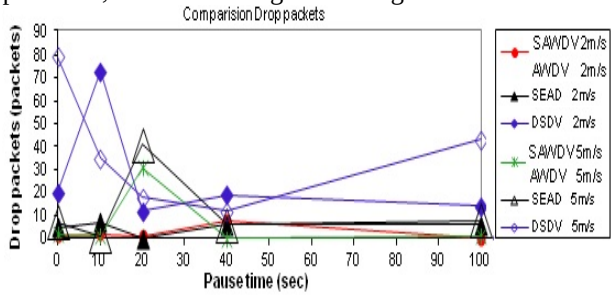

Fig.16: Drop Packets at SIMT 100s with 2 & 5m/sec

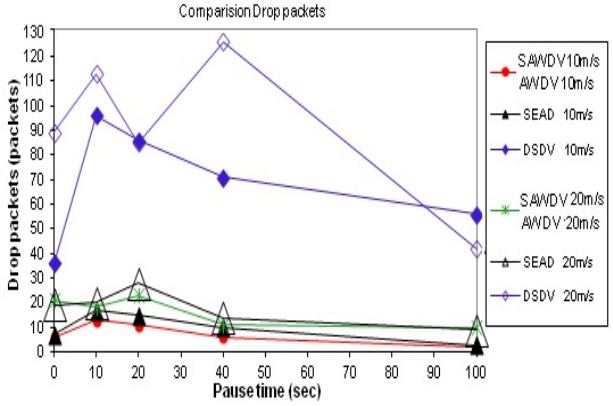

Fig.17: Drop Packets at SIMT 100s 10 & 20m/sec

It is obvious that the proposed SAWDV routing protocol demonstrates lower packet dropping by malicious node attacks, because it prevents replay, wormhole and modification attacks from injecting in the MANETs. Thus the proposed SAWDV enhanced table-driven DSDV provides a solution for possible packet-dropping attacks in mobile ad-hoc networks.

6. Security Analysis of Routing Protocols

6.1. Computational Complexity

The SEAD routing protocol is efficient in terms of the metric of average end-to-end delay of packet delivery and the Complexity processing time compared with the proposed SAWDV and AWDV routing protocols, which is significantly higher as shown in Fig.18. But the DSDV routing protocol has lower CPU processing time compared with both, because the authenticated digital watermarking algorithm of proposed a SAWDV routing protocol consuming lower execution prepared sum of delays at HMS, than compared with the SEAD routing protocol using one way hash chains are consumed very fast execution algorithm.

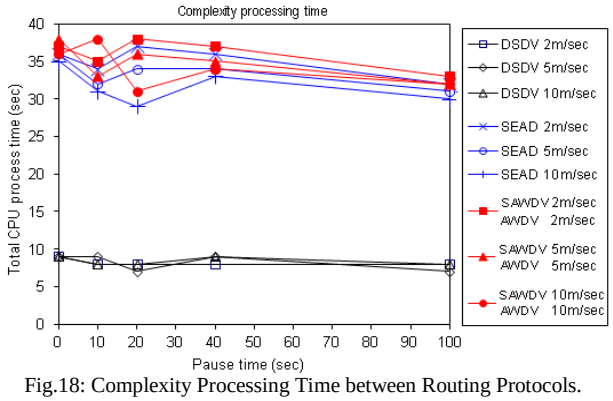

Fig.18: Complexity Processing Time between Routing Protocols.

6.2. Security Analysis

The SAWDV, AWDV and SEAD routing protocols were developed based on DSDV protocol. The SEAD incorporates One-Way hash function, to authenticate during the routing update mechanism. But the proposed SAWDV and AWDV routing protocols incorporates digital watermarking to authenticate during the routing update mechanism in order to enhance the routing security. From the previous section of the performance evaluation, we have seen the good performance of the traditional DSDV routing protocol with LMS and small scalability of network (number of nodes). Thus the proposed SAWDV routing protocol shows the result of the performance metric in the packet delivery ratio is a higher value, indicating that most of the packets are being delivered to the destination. The SAWDV thus performs well when compared with the traditional

DSDV routing protocol, with significant improvement in terms of packet delivery ratio compared with the SEAD routing protocol at a lower mobility 2, 5 and 10 m/sec, with guards against malicious node attacks and attempts to cause other nodes to consume excess network bandwidth or processing time by applying route spoofing. Fabricated routing updates cannot be injected into the network; routing messages cannot be altered in transit; routing loops cannot be formed through malicious node action and routes cannot be redirected from the shortest path by malicious node action. Table.2 shows a comparative security analysis between routing protocols, the DV routing protocol cannot defend against attacks, for instance, creating routing loops, but in DSDV, the main contribution of the algorithm was to solve the routing loop problem occurred by stale routing, including a parameter called destination sequence number. From above table show that some types of security attacks are possible in the DSDV, SEAD and AWDV protocols with a set of compromised nodes in simulated attack environments. The routing loops are possible only when there is more than one malicious node in the network. Thus confidentiality, availability, and integrity of the network topology with respect to participating nodes are maintained through authentication with neighboring nodes.

Table.2: Comparative Security Analysis between Routing Protocols.

Attack patterns	**SAWDV**	**AWDV**	**SEAD**	**DSDV**
Replay	Yes	Yes	Yes	Yes
Denial of service	Yes	Yes	Yes	No
Impersonation or spoofing	Yes	Yes	Yes	No
Routing tables overflow	Yes	Yes	Yes	No
Byzantine	Yes	Yes	Yes	No
Wormhole	**Yes**	No	No	No
Modification	**Yes**	No	No	No
Vertex cut	No	No	No	No

The SAWDV is robust against uncoordinated attack patterns through neighbor authentication. A malicious node may not impersonate another node while sending the control packets to create an anomalous update in the routing table. Rather, the proposed SAWDV, AWDV and SEAD routing protocols do not allow for new nodes to join the network because the proposed SAWDV routing protocol is a hidden watermark, and the source Ethernet address of the owner node (sender) is in the watermarked packet, preventing impersonation from any malicious node. Likewise with routing table overflow attacks, as the attacker attempts to create routes to nonexistent nodes with the SAWDV, AWDV and SEAD routing protocols. Whereas the wormhole attacks are possible in SEAD and AWDV routing protocols because if the attacker records a packet (routing information (destination address node and hash value)) at one location on the network, and retransmits the recorded data into the network, it disrupts the routing information. However, the proposed SAWDV routing protocol is robust, because it uses watermarked packet content, the hidden routing information (the source Ethernet address (owner address of the source node sender) and secure watermark) to prevent wormhole attacks being injected into the network. Modification attacks are also possible in AWDV and SEAD routing protocols. If malicious nodes can easily modify routing information, network traffic could be dropped by being redirected to a different destination or could take a longer route to the destination, cause increasing communication delays. If a noise tunnel in transmutation, some change in routing information (hash value) or any other modified in hash value could occur due to routing disruption, thus cause network traffic to be dropped. Then the malicious nodes can easily divert traffic and cause denial of service simply by altering these fields. But the proposed SAWDV routing protocol is robust against modification attacks because it hides hop and source Ethernet address of the owner node in the watermarked packet to prevent any other modification or manipulation provides integrity, where AWDV cannot prevent any other modification because it is hide only number of hops to reach the destination in the watermarked packet. The SAWDV, AWDV and SEAD routing protocols are also robust against replay attacks, when it is using old route advertisements that can be sent to a node causing it to update its routing table with stale routes. It might then updates its routing table with stale routes, causing a routing disruption. This problem does not occur in the proposed SAWDV routing protocol, which requires matching between the source Ethernet address of the owner node, received by the sender, within the source Ethernet address of the owner node hidden in the received watermarked packet, then required to authenticate. On the other hand each node in the DSDV routing protocol tracks, for each destination, the average time between when the node receives the first update for some new sequence number for that destination and when it receives the best update for that sequence number for it (with the minimum metric among those received with that sequence number). When deciding to send a triggered update, each DSDV routing protocol delays any triggered update at destination node, to selecting route with the best metric for that sequence number. Conversely, the SAWDV, AWDV and SEAD routing protocols do not use such a delay (an average weighted settling time in sending triggered updates) to reduce the number of redundant triggered updates to prevent malicious node attacks or attempts on the nodes in MANETs that might maliciously not use the delay, and to reduce the process CPU time. Finally, the DSDV routing protocol cannot defend against any kind of attacks and the SAWDV, AWDV and SEAD routing protocols cannot defend against vertex cut attacks. Moreover the proposed SAWDV routing protocol is

robust enough against multiple uncoordinated attacks as shown in Table 2 and it is not resource-intensive, and developing the protocol is easy to implement

7. Conclusion

The main objective of this paper improves the AWDV to provide a secure routing protocol called SAWDV: Secure Authentication Watermarking in Ad-hoc Destination-Sequenced Distance-Vector routing protocol and compared with traditional DSDV and with AWDV and SEAD as a secure routing protocols.

In this paper, we have studied the results of the simulation models by using ns-2 simulator, which are showed the effect under various pause times with different simulation run time and different movement mobility, over all we are suggesting that the SAWDV outscores the traditional DSDV, SEAD and AWDV routing protocols in all aspects and the proposed SAWDV routing protocol demonstrate in all aspects of results with the same outscores in AWDV routing protocol. Moreover, the improving security of AWDV routing protocol by (embedding public watermark, hiding the owner address of the source node (sender), and the number of hops to reach the destination node) in a "watermarked packet" at each authenticated routing update to prevent multiple uncoordinated wormhole and modification attacks in the term of drop packets.

The performance of the SAWDV is suggest robust enough against multiple uncoordinated attacks, in the (replay, wormhole, modification, byzantine and denial of service) attacks, with compared of the SEAD and AWDV protocols but it cannot defend against the wormhole and modification attacks. Whereas, the SAWDV under the performance AED metric of packet delivery the authenticated digital watermarking algorithm “consuming lower execution algorithm” prepared delay authentic routing update produced significantly higher routing overhead than compared with of the SEAD using one way hash chains “consumed very fast execution algorithm”. The DSDV has worse performance than either of the others and worst simulated performance at the higher mobility of 20m/s, because it is not adaptive to the route changes that occur, but, only defend against replay attack. Furthermore, the SAWDV, AWDV and SEAD routing protocols cannot defend against vertex cut attacks. Likewise, from the performance results the SAWDV enhanced table-driven routing protocol DSDV provides the solution for the possible packet dropping attacked in MANETs.

References

[1] S. A. Mahdi, M. Othman, H. Ibrahim, J. Md. Desa and J. Sulaiman, "Protocols for Secure Routing and Transmission in Mobile Ad-Hoc Network", Journal of Computer Science Vol.9, No.5, pp.607-619, 2013.

[2] A.F.A. Abidin, N.S.M. Usop and M.K. Yusof, "Performance Comparison of Wireless Ad-Hoc Routing Protocols", International Journal on Computer Science and Engineering, Vol.3, No.1, pp.216-224, Jan. 2011.

[3] S. Goudarzi, A. H. Abdullah, S. Mandala, S. A. Soleymani, M. A. R. Baee, M. H. Anisi, and M. S. Aliyu "A Systematic Review of Security in Vehicular Ad-hoc Network", the 2nd Symposium on Wireless Sensors and Cellular Networks (WSCN'13), Jeddah, Saudi Arabia, pp.1-10, December 13-16, 2013.

[4] M. Gunasekaran and K. Premalatha " SPAWN: a secure privacy-preserving architecture in wireless mobile ad-hoc networks", Springer in EURASIP Journal on Wireless Communications and Networking, pp.1-12, 2013.

[5] P. M. Jawandhiya, M. M. Ghonge, M.S.Ali and J.S. Deshpande," A Survey of Mobile Ad-hoc Network Attacks", Inter. Journal of Engineering. Science and Technology, Vol.2, No.9, pp.4063-4071, 2010.

[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 Engineering, Kuttippuram, Kerala, India, pp.49-54, Dec 14-15, 2007.

[7] M. B. Aliwa, T. El-A. El-Tobely, M. M. Fahmy, M. EL Said Nasr and M. H. Abd El-Aziz, "A Novel Authenticated Digital Watermarking in Mobile Ad-hoc Networks Using ns-2 Simulator ", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.4, pp.44-55, April 2011.

[8] 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. & Applications, IEEE Computer Society, Callicoon, NY, USA, pp.3-13, 2002.

[9] 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 Appli., NY, USA, Vol.24, No.4, pp.234–244, Oct. 1994.

[10] G. Kaur and K. Kaur, "Digital Watermarking and Other Data Hiding Techniques", International Journal of Innovative Technology and Exploring Engineering, Vol.2, No.5, pp.181-183, April 2013.

[11] 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, 2010.

[12] 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, pp.227-240, August 30, 2009.

[13] A. hashad and M. Gannan, "Performance evaluation of routing protocols for mobile ad-hoc network ", ICCTD Inter. Conf. on Comp. Tech. & Development, IEEE Comp. Society, Malaysia, pp.1-10, 13-15 November 2009 .

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

[15] K. Varadhan, "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, pp.1-413, generating traffic pattern files, page.160, 23August 2006.

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

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

[18] 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.

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

[20] 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, pp.538-544, 2008.

[21] G. Fang, L.Yuan, Z. Qingshun and Li Chunli, "Simulation and Analysis for the Performance of the Mobile Ad-Hoc Network Routing Protocols", IEEE 8th International Conference on Electronic Measurement & Instruments, Xian International Convention Center, Xian, China, Vol.2, pp.571-575, 16-18 Aug. 2007.

Mehemed Bashir Aliwa was born in Misurata, Libya, in 1969. He received the Ph.D. degree from the Electrical Engineering (Computer and Control Engineering) Department of the Faculty of Engineering TANTA University, Egypt, in 2012, 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, and B.Sc. Degree in Computer Engineering on 1992 from the Engineering Academy, Tajoura-Libya. Regard to my works, from 1992 to 1996 a research center of military industrialization, from 1996 to 1997 a Lecturer at the military School of Electronic Support and from 1997 to 2005 a director office of the global information network and the office of training and maintenance in computer system in Authority operations and training course Libyan armed forces. Currently, I am getting a training course of Oracle Database Administration and Developer in EMAK International Academy an Oracle Academy, Cairo, Egypt. I am interested research includes digital watermarking, hiding information, and routing protocol in mobile ad-hoc networks.