ISSN 2348 – 9928
IJAICT Volume 6, Issue 2, February 2019 Doi:01.0401/ijaict.2015.05.04 Published on 05 (2) 2019

COMPARISON OF SEAD AND DSDV UNDER VARIOUS ATTACKS

Mr. Ranjeet Yadav, B.Tech, M.Tech, (PhD),(PGDDM)
Assistant Professor,
DBRAIT Port Blair

Abstract— This paper describes how security feature is important in ad hoc network. In this paper we illustrate DSDV routing protocol and Secure Efficient Ad hoc Distance vector routing protocol (SEAD), based on the design of the Destination-Sequenced Distance-Vector routing protocol. Various attacks are introduced in the network scenario such as Denial-of service Attack, Flooding Attack and Wormhole attack. Using ns-2 and DSDV protocol the results of the original DSDV is compared to the SEAD under attack and without attack. The simulation results verify that the extended schemes which use DSDV as the underlying protocol provides substantial security over the DSDV. SEAD performs well over the range of scenarios we tested, and is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of any active attackers or compromised nodes in the network.

Keywords— DSDV-Destination-Sequenced Distance-Vector routing protocol, SEAD- Secure Efficient Ad hoc Distance vector routing protocol, ns2-Network Simulator

I. INTRODUCTION

Due to the unique characteristics of ad hoc wireless networks, networks are highly vulnerable to security attacks compared to wired networks or infrastructure-based wireless networks. The role of the routing protocol in an ad hoc network is to allow nodes to learn multihop paths. Since the nodes in the network may move at any time, or may even move continuously, and since sources of wireless interference and wireless transmission propagation conditions may change frequently, the routing protocol must also be able to react to these changes and to learn new routes to maintain connectivity.

Secure ad hoc network routing protocols are difficult to design, due to the generally highly dynamic nature of an ad hoc network and due to the need to operate efficiently with limited resources, including network bandwidth and the CPU processing capacity, memory, and battery power (energy) of each individual node in the network.

Existing insecure ad hoc network routing protocols are often highly optimized to spread new routing information quickly as conditions change, requiring more rapid and often more frequent routing protocol interaction between nodes than is typical in a traditional (e.g., wired and stationary) network. Routing protocols for ad hoc networks generally can be divided into two main categories: *Periodic Protocol* and *on-demand Protocol*. In periodic nodes periodically exchange the routing information with other node in an attempt to have each node always know a current route to all destinations. In an on-demand (or Reactive protocol) node exchange the routing information only when needed with a node attempting to discover a route to some destination only when it has a packet to send to that destination. Each style of ad hoc network routing protocol has its on advantage and disadvantages. In this paper we focus on securing ad hoc network routing using periodic protocol (or proactive) protocol in general using Distance vector routing protocol.

1.1 Wireless Ad hoc network

A wireless Ad hoc network has many advantageous when compared to its wired counterpart, such as rapid deployment without complicated configuration. It can also be used in those environments where it is difficult to set up wired networks like in military fields or emergency (fire, safety, and rescue) scenes. In wireless Ad hoc networks security is a huge concern because most of the routing protocol is based on finding the shortest path to the destination mobile nodes. Thus developing a method for secure routing protocol while maintaining network connectivity and finding the shortest path possible for the destination node in an ad hoc network. The lack of any centralized infrastructure in mobile ad hoc networks (MANET) is one of the greatest security concerns in the deployment of wireless networks. Thus communication in MANET functions properly only if the participating nodes cooperate in routing without any malicious intention. However, some of the nodes may be malicious in their behaviour, by indulging in flooding attacks on their neighbors. Some others may act malicious by launching active security attacks like denial of service. In addition, the wireless medium exposes any message transmission to anyone located within the communication range, a specific type of emerging security threat known as the wormhole attack.

1.2 Objective

The focus of this paper is to introduce new methodologies for security in Ad hoc network. Secure ad hoc network routing protocols are difficult to design, due to the generally highly dynamic nature of an ad hoc network and due to the need to operate efficiently with limited resources, including network bandwidth and the CPU processing capacity, memory, and battery power (energy) of each individual node in the network. Existing insecure ad hoc network routing protocols are often highly optimized to spread new routing information quickly as conditions change, requiring more rapid and often more frequent

routing protocol interaction between nodes than is typical in a traditional (e.g., wired and stationary) network.

In this paper we tested the scenario under various attacks and without attack for DSDV and SEAD routing protocol.

II. NETWORK SECURITY REQUIREMENTS IN AD HOC NETWORK OVERVIEW

A security protocol for ad hoc wireless networks should satisfy the following requirements:

***Confidentiality*:** The data send by the sender must be comprehensible only to intended receiver.
***Integrity*:-**the data sent by the source node should reach the destination node as it was sent (unaltered).
***Availability*:** The network should operational all the time. It must be robust enough to tolerate link failures and also be capable of surviving various attacks mounted on it. It should provide guaranteed service whenever an authorised user requires them.
***Non-repudiation*:** It is a mechanism to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

The ultimate goal of the security solution for ad hoc network is to provide security services such as authentication, confidentiality, integrity, anonymity, and availability to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack. To protect the network connectivity between the mobile nodes over potentially multihop wireless channels, which is the basis to support any network security services. Multihop connectivity is provided through two steps: (1) ensuring one-hop connectivity through link-layer protocol and (2) extending connectivity to multiple hops through network-layer routing and data forwarding protocols.

From the security design perspective is the lack of a clear line of defense in ad hoc wireless. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a routers, each mobile node in an ad hoc network may function as a router and forward the packets for each other node. The wireless channel is accessible to both legitimate network users and malicious attackers. There is no well defined place where traffic monitoring of access control mechanism can be deployed. As a result, the boundary that separate the inside network from the outside world becomes blurred. The existing ad hoc routing protocols, such as Ad Hoc On Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) , and wireless MAC protocols, such as 802.11, typically assume a trusted and cooperative environment. As a result, a malicious attacker can readily become a router and disrupt network operations by intentionally disobeying the protocol speciation.
There are basically two approaches to protecting MANETs: protective approach and reactive approach. The proactive approach attempts to prevent an attacker from launching attacks in the first place, typically through various cryptographic techniques. In contrast, the reactive approach seeks to detect security threats and react accordingly. Due to absence of a clear line of defense, a complete security solution should integrate both approaches and encompass all three components: prevention, detection and reaction.
In this paper we tested the SEAD protocol which is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of active attackers or compromised nodes in the network. We base the design of SEAD in part on the Destination-Sequenced Distance-vector ad hoc network routing protocol (DSDV), which was designed for trusted environment. In SEAD, we use efficient one way hash functions and do not use asymmetric cryptographic operations in the protocol.

III. CHALLENGES AND ISSUES RELATED TO SECURITY

Designing security protocol for ad hoc network is a difficult and challenging task. This is mainly due to the unique features of the ad hoc network, namely, physical vulnerability, insecure operating environment, shared broadcast radio channel, lack of central authority, and lack of association among the nodes.

Lack of central authority: In wired network and infrastructure-based wireless networks, it would be possible to monitor the traffic on the network through certain important central points (such as routers, base stations and access points) and implement security mechanism at such points. Since in ad hoc network such points are not available these mechanisms cannot be applied.

Lack of association: In ad hoc network at any moment of time a node can join or leave the networks, as a result of dynamic nature of the ad hoc network it is very easy for an intruder to carry out the attack in the network.

Physical vulnerability: Nodes in these networks are usually compact and hand-held in nature. They are vulnerable to theft and could get damaged easily.

Shared broadcast radio channel: In ad hoc network the radio channel is used for communication and is shared among all the nodes in the network. Unlike in wired network a dedicated link for transmission is provided between a pair of end users. A

chance of malicious node to get the data transmitted in ad hoc network is easy. This problem can be minimized to a certain extent by using directional antenna in the network.

Unsafe environment of operation in ad hoc network: The environment of operation is generally not secure where ad hoc wireless networks are used. One important application of such network is in battlefield. In such application nodes may move in and out of hostile and insecure enemy territory, where they would be highly vulnerable to security attacks.

Security is always a desired feature but is attached with strings. When more security features is added into the network, in parallel with the enhanced security strength is the ever increasing computation, communication and management overhead. Consequently, network performance in terms of scalability, service availability, robustness and so on of the security solutions, become an important concern in a resource-constrained ad hoc network. While many contemporary proposals focus on the security vigor of their solutions from the cryptography standpoint, they leave the network performance largely unaddressed. In fact, both dimensions of security strength and network performance are equally important, and achieving a good trade-off between two extremes is one fundamental challenge in security design for ad hoc network.

One fundamental vulnerability comes from their open peer-to-peer architecture. Attackers may sneak into the network through the subverted nodes, which pose the weakest link and incur a domino effect of security breaches in the system. The wireless medium and node mobility poses far more dynamics in MANETs compared to the wired medium. The network topology is highly dynamic as nodes frequently join or leave the network, and roam in the network in their own will. The wireless channel is also subjected to interferences and errors, exhibiting volatile characteristics in terms of bandwidth and delay.

IV. SECURITY ATTACKS IN AD HOC NETWORK

Ad Hoc networks are simple peer-to-peer networks, self-organised with no fixed infrastructure. This leads to new vulnerabilities which are not known in wired networks. The wireless links and dynamic topology definitely gives flexibility in installation. But, at the same time, Security is a major concern in these networks. The wireless channels are vulnerable to various security attacks. Some of the ad hoc nodes may be victimized in the network by malicious nodes and may indulge in various denial-of-service attacks. The lack of security frameworks in these networks are one of the major concerns in their large scale deployments.

In this paper we have discussed the attacks mainly Flooding attack, Wormhole attacks and Denial-of-Service attack.

Flooding: In flooding, each nodes which receives a packet broadcasts it if the maximum hop-count of the packet is not reached and the node itself is not the destination of the packet. Most of the reactive protocols are prone to flooding attack by repeatedly sending RREQ or garbage DATA packets to different destination some of which never exists. A neighbouring victim node may drain its resources like battery power, processing time by involving itself in the routing traffic. All the nodes in an ad hoc network are categorized as friends, acquaintances or strangers based on their relationships with their neighboring nodes. During network initiation all nodes will be strangers to each others. A estimator is used in each node to evaluate the trust level of its neighboring nodes.

Wormhole Attack: In this attack, an attacker receives packets in the network and tunnels them to another location in the network, where the packets are resent into the network. This tunnel between two colluding attackers is referred to an wormhole. It could be established through a single long range wireless link or even through a wired link between the two colluding attackers. Due to the broadcast nature of the radio channel, the attacker can create a wormhole even for packets not advertise to itself. Though no harm is done if the wormhole is used properly for efficient relaying of packets, it puts the attacker in a powerful position compared to other nodes in the network, which the attacker could use in a manner that could compromise the security of the network. If proper mechanisms are not employed to defend the network against wormhole attacks, most of the existing routing protocols for ad hoc wireless networks may fail to find valid routes.

For DSDV, if each routing advertisement sent by node A were tunnelled to node B, and vice versa, then A and B would believe that they were neighbors. If they were not within wireless transmission range, they would be unable to communicate.

Furthermore, if the best existing route from A to B were at least 2n + 2 hops long, then any node within n hops of A would be unable to communicate with B, and any node within n hops of B would be unable to communicate with A. Otherwise, suppose C were within n hops of A, but had a valid route to B. Since A advertises a metric 1 route to B, C would hear a metric n + 1 route to B. C will take that route if it is not within n + 1 hops of B, in which case there would be a n-hop path from A to C, and a n + 1-hop path from C to B, contradicting the premise that the best real path from A to B is at least 2n + 2 hops long.

V. DESTINATION SEQUENCED DISTANCE VECTOR (DSDV) PROTOCOL

The destination sequenced distance vector routing protocol is a proactive routing protocol. This protocol adds a new attribute, sequence number, to each route table entry at each node. Routing table is maintained at each node and with this table, node transmits the packets to other nodes in the network. This protocol was motivated for the use of data exchange along changing and arbitrary paths of interconnection which may not be close to any base station.

5.1 Protocol Overview

Each node in the network maintains routing table for the transmission of the packets and also for the connectivity to different stations in the network. These stations list for all the available destinations, and the number of hops required to reach each destination in the routing table. The routing entry is tagged with a sequence number which is originated by the destination station. In order to maintain the consistency, each station transmits and updates its routing table periodically. The packets being broadcasted between stations indicate which stations are accessible and how many hops are required to reach that particular station. Routing information is advertised by broadcasting or multicasting the packets which are transmitted periodically as when the nodes move within the network. The DSDV protocol requires that each mobile station in the network must constantly advertise to each of its neighbors, its own routing table. Since, the entries in the table my change very quickly, the advertisement should be made frequently to ensure that every node can locate its neighbors in the network. This agreement is placed, to ensure the shortest number of hops for a route to a destination; in this way the node can exchange its data even if there is no direct communication link.

The data broadcast by each node will contain its new sequence number and the following information for each new route: The destination address The number of hops required to reach the destination and the new sequence number, originally stamped by the destination. The transmitted routing tables will also contain the hardware address, network address of the mobile host transmitting them. The routing tables will contain the sequence number created by the transmitter and hence the most new destination sequence number is preferred as the basis for making forwarding decisions. This new sequence number is also updated to all the hosts in the network which may decide on how to maintain the routing entry for that originating mobile host. After receiving the route information, receiving node increments the metric and transmits information by broadcasting. Incrementing metric is done before transmission because, incoming packet will have to travel one more hop to reach its destination .Time between broadcasting the routing information packets is the other important factor to be considered. When the new information is received by the mobile host it will be retransmitted soon effecting the most rapid possible dissemination of routing information among all the cooperating mobile hosts. The mobile host cause broken links as they move form place to place within the network. The broken link may be detected by the layer2 protocol, which may be described as infinity. When the route is broken in a network, then immediately that metric is assigned an infinity metric there by determining that there is no hop and the sequence number is updated. Sequence numbers originating from the mobile hosts are defined to be even number and the sequence numbers generated to indicate infinity metrics are odd numbers. The broadcasting of the information in the DSDV protocol is of two types namely: full dump and incremental dump. Full dump broadcasting will carry all the routing information while the incremental dump will carry only information that has changed since last full dump. Irrespective of the two types, broadcasting is done in network protocol data units (NPDU).

Full dump requires multiple NPDU's while incremental requires only one NPDU to fit in all the information. When an information packet is received from another node, it compares the sequence number with the available sequence number for that entry. If the sequence number is larger, then it will update the routing information with the new sequence number else if the information arrives with the same sequence number it looks for the metric entry and if the number of hops is less than the previous entry the new information is updated (if information is same or metric is more then it will discard the information). While the nodes information is being updated the metric is increased by 1 and the sequence number is also increased by 2. Similarly, if a new node enters the network, it will announce itself in the network and the nodes in the network update their routing information with a new entry for the new node. During broadcasting, the mobile hosts will transmit their routing tables periodically but due to the frequent movements by the hosts in the networks, this will lead to continuous burst of new routes transmissions upon every new sequence number from that destination. The solution for this is to delay the advertisement of such routes until it shows up a better metric.

DSDV requires a regular update of its routing tables, which uses up battery power and a small amount of bandwidth even when the network is idle. Whenever the topology of the network changes, a new sequence number is necessary before the network re-converges; thus, DSDV is not suitable for highly dynamic networks. (As in all distance-vector protocols, this does not perturb traffic in regions of the network that are not concerned by the topology change). Wastage of bandwidth due

to unnecessary advertising of routing information even if there is no change in the network topology .DSDV doesn't support Multi path Routing. It is difficult to determine a time delay for the advertisement of routes. It is difficult to maintain the routing table's advertisement for larger network. Each and every host in the network should maintain a routing table for advertising. But for larger network this would lead to overhead, which consumes more bandwidth.

VI. SEAD: SECURE EFFICIENT DISTANCE VECTOR ROUTING FOR MOBILE WIRELESS AD HOC NETWORKS

Secure efficient ad hoc distance vector (SEAD) routing protocol [1] ,is a secure ad hoc routing protocol based on the DSDV routing protocol [2]. This protocol is mainly designed to overcome security attacks such as DoS and resource consumption attacks. The operation of the routing protocol does not get affected even in the presence of multiple uncoordinated attackers corrupting the routing tables. The protocol uses one way hash function and does not involve any asymmetric cryptographic operation.

One-Way Hash Function

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 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 output of the hash function. The function H should be simple to compute yet must be computationally infeasible in general to invert. A more formal definition of one-way hash functions and a number of such functions have been proposed, including MD5 and SHA-1.

To create a one-way hash chain, a node chooses a random initial value $x \in \{0,1\}^{\rho}$ and computes the list of values

$h_0, h_1, h_2, h_3, \ldots ; h_n$

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 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 h_{i-3} by computing $H(H(H(h_{i-3})))$ and verifying that the resulting value equals h_i. To use one-way hash chains for authentication, we assume some mechanism for a node to distribute an authentic element such as h_n from its generated hash chain. A traditional approach for this key distribution is for a trusted entity to sign public-key certificates for each node; each node can then use its public-key to sign new a hash chain element for itself. PGP like certificates without relying on a trusted public key infrastructure. Alternatively, a trusted node can securely distribute an authenticated hash chain element using only symmetric-key cryptography or non-cryptographic approaches. Since in SEAD, a node uses elements from its one-way hash chain in groups of m, we assume that a node generates its hash chain so that n is divisible by m. When a node first enters the network, or after a node has used most of its available hash chain elements, it can pick a new random x, generate a new hash chain from this x, and send the new generated h_n value to a trusted entity or an alternative authentication and distribution service.

VII. SIMULATION EVALUATION METHODOLOGY

To evaluate the performance impact of our security approach in SEAD without attackers, we modified the DSDV-SQ implementation in our extensions to ns-2. Specifically, we increased the size of each routing update to represent the authentication hash value in each table entry. We also removed the settling time and the sequence number changes. Because we wanted to determine the cost of SEAD without significant additional assumptions, we simulated pair-wise shared key authentication. For example, if nodes are loosely time synchronized, an upper bound on the maximum sequence number can be easily determined. Alternatively, intrusion detection techniques can be used to avoid the need to authenticate many bogus up- dates. In particular, a node can check the neighbor authentication very easily. If certain neighbors persist in sending updates with bogus metric authenticators, those neighbors can be ignored, or the verification of their updates can be relegated to a lower priority.

We chose the ns-2 simulator for this study because it realistically models arbitrary node mobility as well as physical radio propagation effects such as signal strength, interference, capture effect, and wireless propagation delay. Our propagation model is based on the two-ray ground reflection model. The simulator also includes an accurate model of the IEEE 802.11 Distributed Coordination Function (DCF) wireless MAC protocol.

In our simulations, nodes moved according to the random waypoint mobility model. Each node is initially placed at a random location and pauses for a period of time called the pause time; it then chooses a new location at random and moves there with a velocity randomly chosen uniformly between 0 and the maximum speed Vmax. When it arrives, it repeats the process of

pausing and then selecting a new destination to which to move. The data communication pattern in our study uses 20 source-destination pairs, each sending a Constant Bit Rate (CBR) flow of 4 data packets/s. Each data packet is 512 bytes in size. Table details the parameters used in our simulations.

TABLE 7.1: PARAMETERS FOR SEAD PERFORMANCE

Scenario Parameters	
Number of Nodes	50
Maximum Velocity Vmax	20 m/sec
Dimension of Space	1500x300 m^2
Nominal radio range	250 m
Source-destination pair	20
Source data rate (each)	4 packets/sec
Application Data payload size	512 bytes/sec
Total application data load	327 KB/sec
Raw physical link bandwidth	2Megabytes/sec
SEAD parameters	
Periodic Route update interval	15 sec
Periodic updates missed before link is declared broken	3
Maximum Packets buffered per node per destination	5
Hash Length (ρ)	80 bits

We evaluated SEAD by comparing it to DSDVSQ. We measured performance along three metrics:

• ***Packet delivery fraction***:

The total no of packet received, divided by total no of packet originated.

•***Routing load overhead:***

The total no of packet received by the total no of packets including control packets

• ***Average End to End delay:***

The time from source the packet is sent to the packet reach the destination.

7.1 Simulation Results

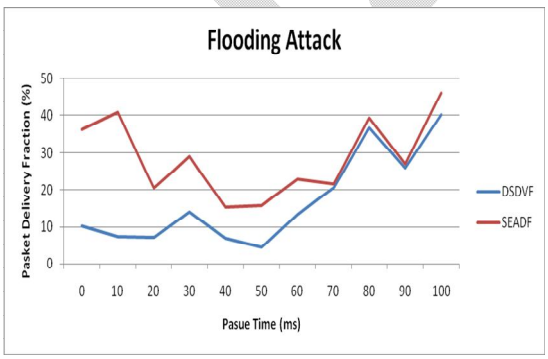

Figure (a) : PDF for Flooding Attack

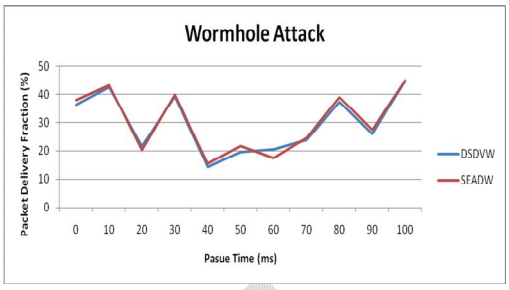

Figure (b) : PDF for Worm-hole Attack

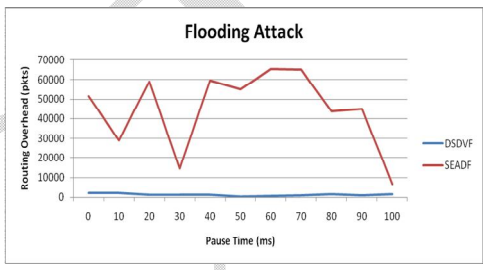

Figure (c) : Routing Overhead for Flooding Attack

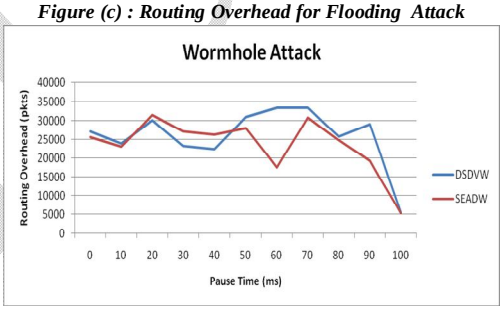

Figure (d) : Routing Overhead for Wormhole Attack

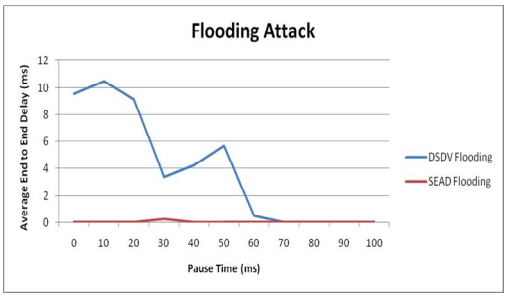

Figure (e) : Average End to End Delay for Flooding Attack

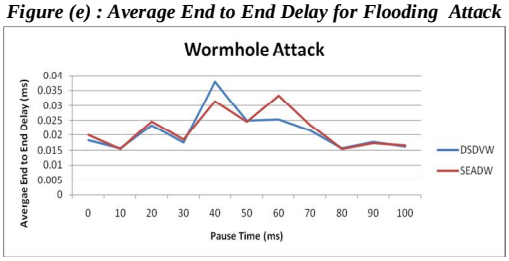

Figure (f) : Average End to End Delay for worm-hole Attack

The packet delivery fraction for SEAD and DSDV-SQ as shown in fig a & b, SEAD consistently outperforms DSDV-SQ in terms of packet delivery fraction. By not using a weighted settling time delay in sending triggered updates in SEAD, the number of routing advertisements sent by SEAD generally increases relative to DSDV-SQ, allowing nodes to have more up-to-date routing tables.However, SEAD also increases overhead, both due to this increased number of routing advertisements, and due to the increase in size of each advertisement from the addition of the hash value on each entry for authentication. This increased overhead is shown in figures d & e, which show the number of routing overhead packets caused by the two protocols in these same simulations. The increased overhead in SEAD causes some congestion in the network.

VIII. CONCLUSION

In this paper the performance of the SEAD, a new secure ad hoc network routing protocol using Distance Vector Routing Protocols is evaluated by using the network simulator (NS2). Many previous routing protocols for ad hoc networks have been based on distance vector approaches, but they have generally assumed a trusted environment. Instead, in designing SEAD, an inexpensive cryptographic primitive to each part of the protocol functionality to create an efficient, practical protocol that is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of active attackers or compromised nodes in the network. Together with existing approaches for securing the physical layer and MAC layer within the network protocol stack, the SEAD protocol provides a foundation for the secure operation of an ad hoc network.

The performance evaluation study of SEAD and DSDV-SQ routing protocols are compared in terms of their performance parameters such as Packet delivery fraction, Average end to end delay and Routing load overhead as a function of pause time in the random waypoint mobility model. The Packet delivery fraction for SEAD is much better under DoS attack as compared to wormhole and flooding attacks whereas DSDV underperforms in all the above attacks. However for the above attacks average end to end delay and Routing load overhead is more for SEAD when compared to DSDV.

The Routing load overhead under wormhole attack for both SEAD and DSDV is getting decreased at higher pause time this is due to tunnelling of the node due to decrease in mobility of node at higher pause time, whereas under flooding attack SEAD overhead increases with increase in pause time since it floods the packets at the neighbor node due to decrease in mobility at higher pause time and making each node highly vulnerable with number of packets. For wormhole attack the average end to end delay for both SEAD and DSDV is decreases at higher pause time, whereas for flooding attack SEAD delay is increases at higher pause time due to decreased available network capacity from the increased overhead. SEAD actually outperforms DSDV-SQ in terms of packet delivery ratio, although it does create more overhead in the network, both due to an increased in size of each advertisement due to the addition of the hash value on each entry for authentication. At all pause times, SEAD exhibits higher latency than DSDV due to decreased available network capacity from the increased overhead in SEAD. The rise in delay is due to non uniform distribution of nodes in space caused by node motion in random waypoint model.

References

[1] Y.-C. Hu, D.B. Johnson, A. Perrig, Secure efficient distance vector routing in mobile wireless ad hoc networks, in: Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA _02), June 2002, pp. 3–13.

[2] Y.-C. Hu, A. Perrig, D.B. Johnson, Packet leashes: a defense against wormhole attacks in wireless ad hoc networks, in: Proceedings of IEEE Infocomm 2003, April 2003

[3] J.-P. Hubaux, L. Butty_an, S. _CCapkun, The quest for security in mobile ad hoc networks, in: Proceedings of the Third ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2001), Long Beach, CA, October 2001.

[4] Y.-C. Hu, A. Perrig, D.B. Johnson, Ariadne: A secure ondemand routing protocol for wireless ad hoc networks, in: Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), September 2002, pp. 12–23.

[5] S. Basagni, K. Herrin, E. Rosti, D. Bruschi, Secure Pebblenets, in: ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2001), Long Beach, CA, October 2001, pp. 156–163.

[6] S. Kent, C. Lynn, J. Mikkelson, K. Seo, Secure Border Gateway Protocol (S-BGP)—real world performance and deployment issues, in: Symposium on Network and Distributed Systems Security (NDSS_00), February 2000, pp. 103–116.

[7] A. Perrig, R. Canetti, D. Song, J.D. Tygar, Efficient and secure source authentication for multicast, in: Network and Distributed System Security Symposium (NDSS_01), February 2001.

[8] S. Marti, T.J. Giuli, K. Lai, M. Baker, Mitigating routing misbehaviour in mobile ad hoc networks, in: Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000), Boston MA, August 2000, pp. 255–265.

[9] K. Sanzgiri, B. Dahill, B.N. Levine, E. Royer, C. Shields, A secure routing protocol for ad hoc networks, in: Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP_02), November 2002.