On Security Study of Two Distance Vector Routing Protocols for Mobile Ad Hoc Networks

Weichao Wang, Yi Lu, Bharat K. Bhargava

Abstract

This paper compares the security properties of Ad Hoc On-demand Distance Vector (AODV) and Destination Sequence Distance Vector (DSDV) protocols, especially the difference caused by on-demand and proactive route queries, via analysis and simulation of the attacks on them. Through classifying the attacks by their target properties, we explore the potential connections between these properties and the vulnerabilities of the protocols. The analysis shows that the on-demand route query enables the malicious host to conduct real time attacks on AODV with flexibility. We also examine the overhead of conducting attacks, and the propagation and the detection of false routes. It shows that the communication overhead of conducting attacks on DSDV is independent of the attack methods and the width of attack targets. We find that a single false route propagates slower in AODV than in DSDV. The analysis also shows that the detection of false destination sequence attacks in AODV heavily depends on the mobility of hosts while in DSDV it is not. False distance vector and false destination sequence attacks are studied by simulation. Two connection scenarios: common destination and uniformly distributed traffic load, are considered. The delivery ratio, communication overhead and the propagation of false routes are measured by varying the number of connections and the maximum speed of host movement. The simulation results support our analysis by collecting values from practical settings. It is observed that the anomaly patterns of sequence number detected by destination hosts can be applied to detect the false destination sequence attacks.

Index Terms

Ad Hoc Networks, Security Comparison of On-demand and Proactive Properties, AODV, DSDV, Intrusion Detection.

I. Introduction

The emergence of ad hoc networks enables information sharing and network accessing in the area where no fixed infrastructure exists or it is out of the serving range of current cellular systems. But the limited storage and computational capabilities of mobile devices determine their heavy dependence on other hosts for data accessing and information processing. A reliable network topology must be assured through efficient and secure routing protocols for mobile ad hoc networks to enable the pervasive computing.

Many efficient routing protocols for ad hoc networks have been proposed. We may classify them by the time that the routing information is acquired and the methods by which the routes are maintained. In the on-demand (reactive) protocols, such as AODV [1], Dynamic Source Routing (DSR) [2], and Temporally Ordered Routing Algorithm (TORA) [3], the routing information is required and maintained only when it is needed. In the proactive protocols, such as Destination Sequence Distance Vector (DSDV)[4], Clusterhead Gateway Switch Routing (CGSR) [5], and Wireless Routing Protocol (WRP) [6], the hosts exchange the information routinely and construct the routing tables in advance. There are other protocols, such as Zone-based Routing Protocol (ZRP) [7], that employ both mechanisms. A number of studies on performance comparison and optimization for these protocols in attack-free environments have been published [8], [9], [10], [11]. The selected performance measurements include delivery ratio, packet delay, protocol overhead and throughput. They are studied by varying the parameters such as host mobility and traffic load.

Current ad hoc routing protocols assume that the mobile hosts will behave properly and will not introduce malicious information into the systems. However, considering the applying environments of ad hoc networks (battlefields, disaster rescue, etc.), the routing topology is prone to attacks coming from both external and internal. Research has been

The research is supported by CERIAS, NSF grant CCR-0001788 and CISCO URP.

This paper is accepted to appear in the proceedings of IEEE Annual Conference on Pervasive Computing and Communications (PerCom) 2003.

Weichao Wang, Yi Lu, and Bharat K. Bhargava are with the Center for Education and Research in Information Assurance and Security (CERIAS) and Department of Computer Sciences, Purdue University, West Lafayette, IN, 47907, USA. E-mail: wangwc, yilu, bb@cs.purdue.edu

carried out to update and apply the security methods in wired networks to the mobile ad hoc environments. The mechanisms that have been examined include information encryption and user authentication [12] [13]. But these methods face the following difficulties:

- The restriction on power consumption and the limited computational capability of mobile devices prevent the usage of complex encryption algorithms.
- The constantly changing network topology increases the difficulty and overhead of authentication. The dynamic membership puts challenges on the key distribution and management.
- Most importantly, these methods can only guard against external attacks. But the attacks coming from compromised hosts have more severe impacts on performance and network connectivity.

The security and safety properties of ad hoc routing protocols are different from those in wired networks. Therefore, research is required on the vulnerabilities of the protocols, the attacks introduced by them, and their practical impacts on the network performance.

This research provides a detailed analysis on security properties of two ad hoc routing protocols, namely, AODV and DSDV. We especially examine the difference caused by on-demand and proactive mechanisms, which is the primary difference between the two protocols. The research enables us to ascertain the potential connections between the vulnerabilities and these properties, instead of a specific protocol. Many properties, such as distance vector, and destination sequence, are also adopted by other ad hoc routing protocols. Thus the results can be applied beyond AODV or DSDV and provide guideline for the design of a secure routing protocol and the Intrusion Detection Systems (IDS) for ad hoc networks.

The remainder of this paper is organized as follows: Section II presents the related work. Section III presents an overview and characterization of AODV and DSDV. Section IV exploits some attacks on the two protocols and presents the security comparison. It classifies the attacks by their target properties and especially compares the security deficiencies caused by on-demand route query and the proactive mechanism. Section V illustrates the damages in practical settings. It collects the impacts of false distance vector attacks and false destination sequence attacks by simulation. We find that a considerable part of the hosts are cheated by the false routes and it may drastically lower the performance on delivery ratio. The communication costs of the attacks against the network traffic load and host mobility are studied. Section VI presents the anomaly patterns of sequence number that can be used in the detection of false destination sequence attacks. Section VII concludes the paper.

II. Related Work

Besides the studies on performance comparison, there are efforts, in both theory analysis and project development, to investigate the security of ad hoc networks, to establish IDS, and to construct secure communication protocols.

Zhang and Lee studied the characters of ad hoc networks related to security and exploited the difficulties to apply current IDS to the wireless environments [14]. The authors presented a generic multi-layer integrated IDS for the ad hoc networks. But the solutions to some critical problems, such as how to efficiently collect the patterns of attacks, and how to safely distribute the intrusion detection results to other hosts, are not discussed in detail. Bhargavan, Zhou and Haas explored the security issues of wireless LANs and ad hoc networks [15] [16]. They summarized the primary questions to achieve security and the challenges to the routing protocols. The discussion is restricted at a high level and did not dig deeply into protocols.

Several protocols have been established to protect the network layer in a mobile ad hoc network. The researchers at UCLA have built a self-organized network-layer security mechanism to enable the neighbors to monitor the behaviors of a specific host [17]. Hubaux and his colleagues established a public key management mechanism in mobile ad hoc networks [18]. It presents a practical solution for the key management problem stated by Haas in [15]. The evaluation of secure routing in ad hoc networks can be found in [19]. Other security analyses and IDS structures have been presented in [20], [21], [22], [23]. But no security comparison conclusions based on quantitative results have been reached.

Several projects are underway to develop secure communication or build IDS for ad hoc networks [24], [25], [26], [27]. The technologies that have been adopted include sending data through multi-path to increase reliability, and monitoring traffic distribution to avoid DoS attack. These mechanisms will increase both computation and communication overhead during the normal operation period of the network, which will affect the performance. Our research emphasis differs from theirs by focusing more on the protection of routing protocols.

III. Description of Protocols

A. Introduction of DSDV

DSDV is one of the first routing protocols designed for ad hoc networks. It is based on distance vector technology. Every host will broadcast its routing table routinely to its direct neighbors, which enables the proactive route discovery. When one link change that may severely impact the connectivity happens, a partial update can also be sent. The neighbors will recalculate the available paths to other hosts and update their routing tables. To avoid the routing loop, DSDV applies destination sequence number to identify the freshness of the routing information. The sequence number of a specific host is increased at every time when the host sends out the route update. The route with larger sequence number is always preferred. When multiple paths with the same destination sequence are available, the shortest one will be selected. More details about DSDV can be found in [4].

DSDV's desirable features are its short delay of connections brought by proactive route discovery and the easiness of implementation. Because every host has to maintain a routing table that covers all hosts in the network, DSDV does not scale well to large ad hoc networks. The overhead of recalculation of routes and periodically packet exchanges consumes the valuable resource of energy and bandwidth. However, the proactive mechanism sets up difficulties for the malicious hosts to conduct attacks. This will be shown by the analysis and simulation results presented later.

B. Introduction of AODV

AODV is a reactive protocol that computes routes solely on-demand. It is based on distance vector technology. The mobile hosts only maintain the next hop to every destination. When the source host wants to send packets to the destination and cannot get the route from its routing table, it will broadcast a Route Request (RREQ) throughout the network. The receivers may establish the routes back to the source host through the paths that they first get the RREQ. If the receiver has an active route to the destination, it will unicast a Route Reply (RREP) back to the source. Otherwise, the RREQ will be re-broadcast further. If a reply is sent, all hosts along that path may establish the route to the destination through this packet. Because there may exist multiple exclusive paths between two hosts, a mobile host can receive the same RREQ more than once. To prevent the same request from being broadcast repeatedly and consuming the bandwidth, every request is uniquely identified by a <Host ID, Broadcast ID> couple. Every host keeps a record for the RREQs that have been processed. The mobile hosts send out the Route Error (RERR) packets to their neighbors to report broken paths and activate the route re-discovery procedure.

To avoid routing loop and identify the freshness of the route, destination sequence number is introduced. The sequence of a mobile host is increased at every time that it sends RREQ or RREP. A larger sequence number always implies a fresher route. The sequence number is carried in both RREQ and RREP. The sequence in RREP must be larger than or equal to the one carried in corresponding RREQ to avoid the source host to adopt a stale path. When more than one path represented by different RREPs are available, the one with the largest destination sequence number is always preferred. If several paths have the same sequence, the shortest one will be chosen. More details about AODV can be found in [1].

AODV's desirable features are its low byte overhead in relatively static networks and loop free routing using destination sequence numbers. There are improvements in AODV to support multicast [28] and to detect/maintain multiple paths [29]. But the on-demand route query usually brings longer delay for the first few packets. Moreover, it suffers from the problems of route request flooding and the use of MAC level broadcasts. The genuineness of the destination sequence and distance vector leaves vulnerabilities to attackers. These deficiencies introduce the attacks that will compromise the network.

IV. Attack Analysis and Security Comparison

The security deficiencies of ad hoc routing protocols make them vulnerable. We exploit some attacks on AODV and DSDV to expose the potential linkage between the essential features of the protocols and their security flaws. The primary difference between AODV and DSDV is that they work in on-demand and proactive modes separately. It leads to the differences in the attack conduction costs, propagation procedures of false routes, and the detection of attacks in AODV and DSDV when they are under coterminous attacks.

A. Classification of attacks

The attacks can be classified in different ways. Some of them use the sources of the attacks (internal attack, external attack), some are based on the methods through which the attackers acquire control (e.g. buffer overflow, Trojan Horse), and others use the targets of attacks (e.g. file access control, network connectivity). We first divide the attacks into passive and active categories. At a finer level, we group the active attacks by their target features.

1) Passive attacks: A malicious host conducts a passive attack on ad hoc networks by ignoring operations supposed to be accomplished by it. The attacker does not actively initiate malicious actions to cheat other hosts. One example of passive attacks on AODV or DSDV is silent discard, carried on by an intermediate host along the forwarding path. Instead of forwarding a packet to the next hop, the attacker drops the data silently. Another example of passive attack is partial routing information hiding. It is conducted by a malicious host in DSDV by hiding the available paths to specific hosts when broadcasting its routing table, or in AODV by ignoring to give out RREP when an active route is available.

It is usually difficult to distinguish passive attacks from Byzantine failures [30] [31] in ad hoc networks. For example, a packet drop can also occur because of host movement or unreliable wireless media. Fortunately, the constantly changing topology and multiple available paths between hosts limit the impacts of passive attacks. For example, in an ad hoc network that has 30 hosts and 25 connections, the silent discard by one malicious host may cause the delivery ratio to decrease 3%. We do not put more efforts on the analysis and detection of passive attacks in this paper because they rely more on the network topology than the protocol characteristics.

2) Active attacks: The malicious host generates an active attack by introducing false information into an ad hoc network. It confuses routing procedures and degrades network performance. In DSDV the false information is carried in the routing packets. In AODV, the RREP is especially attractive to attackers because the reverse routes established by RREQ will become expired in a short time if no active traffic uses those routes. Two active attacks that threat both AODV and DSDV are: false distance vector, and false destination sequence.

- False distance vector attack

Both AODV and DSDV are based on the distance vector technology and the hosts collect routing information solely from direct neighbors. The incomplete understanding of global topology enables the false distance vector attacks. The malicious host forms this attack by claiming that the destination is one (or a few) hop(s) from it in the routing update packets or RREP even if it does not have any available path in its routing table. If no other replies provide a fresher or shorter route, the source will choose the path passing through the malicious host, and the data packets will be dropped or compromised.

- False destination sequence attack

Both AODV and DSDV employ destination sequence to identify the freshness of routing information. When multiple routes are available, the source host always chooses the one with the largest sequence number. By assigning a large false destination sequence in the routing update packets or RREP, the attacker's reply can easily beat other replies and attracts the data traffic. Even worse, the deceived hosts will propagate in good faith the false route to other hosts, thus strengthening the impact of the attack.

B. Security analysis

1) Security comparison: The primary difference between AODV and DSDV is the adoption of on-demand and proactive methods separately. Each of the methods brings advantages and disadvantages in security. While the on-demand route query of AODV enables the low protocol overhead and adaptability to host mobility compared to proactive mechanism, it also leaves a lenient space to the attackers. In proactive protocols such as DSDV the malicious host can send multiple false routes in the same packet. The detailed comparison on security comes as follows:

The on-demand property enables the malicious hosts to conduct real time attacks. Most of the attacks on AODV do not need any preparation or establishment time. For example, when a source host broadcasts RREQ throughout the network, the malicious host may immediately form a false route reply and conduct the attack. As a comparison, when the malicious host tries to attack a proactive protocol, it must send out the false information in advance and has to routinely update the fake route to keep it alive. The longer a false route exists, the larger probability that it is detected. At this point, it is difficult to catch an on-going attack on AODV before it causes performance degradation.

The on-demand property enables the attackers to make flexible choices on the targets, the methods and the points in time of attacks. For example, the malicious host can choose to attack the RREQ coming from a specific source, or it may choose to attack all connections to a particular destination. It can attack the same host with different methods. As to one victim, the attacker can choose to send false replies to some of the routing queries while leaving others untouched. As a comparison, an attack on a proactive protocol usually does not have the flexibility. For example, a false route with a large sequence will be propagated to all other hosts through route exchanges in DSDV. It is difficult for the malicious host to attack a specific connection without impacting others. This stiffness increases the probability that the attacker is detected and located.

It is more difficult to trace back the sources of false information in AODV than in DSDV. As discussed before, the attacks on AODV focus on the RREP packets. The routing reply is unicasted back to the source. Unless the mobile hosts monitor all nearby traffic, there will be only one host along the false route that directly receives the false information from the attacker. For the intruder identification algorithms that use quorum voting to locate the attacker [32] [33], AODV is less efficient on the trace back procedures.

The above analyses provide generic discussion. We specifically compare the communication overhead, the propagation, cancellation and detection of false routes in AODV and DSDV to support our points.

2) Communication overhead of attacks: The communication overhead caused by sending false routes in AODV is highly dependent on the width and frequency of attacks. For example, if the malicious host wants to attack one specific connection, it only needs to send a single false RREP. As the other extreme condition, if the malicious host wants to attack every connection to every other host, it has to send many false RREPs. In DSDV, the overhead is more consistent. The attacker does not have to increase the frequency of sending updates but just carrying more false information in every routing packet. At this point, attacking proactive protocols is more communication efficient for an aggressive attacker.

3) Propagation of false routes: In AODV, the false RREP will be unicasted back to the source host. In [34] it has shown that the average path length is proportional to the square root of host density in ad hoc networks. Therefore the number of hosts cheated by a false RREP is proportional to that order. Considering that an intermediate host may send out RREP to other route query afterwards, the false routes will form a tree rooted at the malicious host. In a proactive protocol, the false routes will be transmitted within a growing round area by the routing exchanges until they are defeated by fresher or shorter routes. At this point, a single false route in AODV propagates slower and has weaker impacts.

4) Cancellation of false routes: As the intrusion detection systems (IDS) in ad hoc networks develop, the malicious host sometimes has to cancel the false routes originated from it to avoid being identified. In most of the ad hoc routing protocols, the updates of current routes are caused either by the break of an active link or the appearance of a fresher or shorter path. The attacker in DSDV can stop sending false routes to cancel the impacts. The new updates will be propagated to the neighbors and the false routes will be smoothly replaced by the real ones. The number of hosts that notice this change depends on the propagation range of the false routes. In AODV when the attacker stops sending packets, the neighbors will assume that the link is broken. The re-discovery procedure will broadcast RREQ throughout the network. At this point, it is more difficult for the attacker in AODV to silently cancel the impacts of false routes.

5) Detection of false routes: It is difficult to detect false distance vector attacks in AODV and DSDV because the hosts only collect routing information from their direct neighbors and cannot construct the global view of the connectivity. The false destination sequence attacks can be detected by the victim if it finds that the sequence has never be generated by it. Because in DSDV the hosts routinely exchange their routing tables, we can estimate the maximum propagation delay of the false sequence from the attacker to the victim by the product of routing packet broadcast interval and their distance in hops. If the false sequence outruns the real number when it arrives at the victim, the attack will be detected. In AODV, the false sequence can be detected only when the false path is broken and the re-discovery procedure broadcasts a RREQ carrying the false number. It depends on the mobility of the hosts and no upper limit can be predicted. More details about the detection of false sequence attacks will be discussed in section VI.

V. Simulation Results

In this section we study the practical impacts of the attacks on ad hoc network performance and examine our analysis through simulation. Two attacks on AODV and DSDV are considered: false distance vector and false destination sequence. Except sending false routes, the attacker will discard any data packets passing through it. We have designed two test conditions to examine their impacts. Under condition one, all connections have the same destination. We measure the delivery ratio, attack overhead and the propagation of false routes when the malicious host attacks the hot point in the network. Under condition two, a more sophisticated traffic scenario is used. We study the delivery ratio and attack overhead against the mobility of the hosts. We first describe the simulation environment, and the two cases will be studied separately.

A. Simulation Environment

The simulation of attacks is deployed using ns2 with CMU extension blocks for ad hoc networks [35]. Table I lists the simulation parameters that we use.

TABLE I

SIMULATION PARAMETERS.

Simulator	ns-2
Examined protocols	AODV, DSDV
Simulated attacks	False distance vector, False destination sequence
Simulation duration	1000 seconds
Simulation area	1000 * 1000 m
Number of mobile hosts	30
Transmission range	250 m
Movement model	Random waypoint
Maximum speed	5 – 20 m / s
Traffic type	CBR (UDP)
Data payload	512 bytes
Packet rate	2 pkt / s
Number of malicious host	1
Host pause time	10 seconds

The choices of the parameters consider both accuracy and efficiency of the simulation. The host moving speed covers a range from human jogging to vehicle riding in country field. Faster speed is not considered because the frequency of route changes will be too high, and confusing the performance degradation caused by attacks. The packet rate of connections is chosen to avoid packet drop caused by congestion even when there are multiple connections converging at the same host.

We choose the following metrics to evaluate the impacts of attacks: (1) packet delivery ratio (2) false routing packets sent by the attacker (3) the number of normal hosts that are cheated by the false routes.

Metric (1) is selected to evaluate the percentage of packets that are affected by the attacks. This can be viewed as the ”strength” of an attack. Metric (2) is used to examine the overhead of different attacks. Here we only consider the cost on communication. If more comprehensive analysis is required, the overhead on computation and storage should also be explored. Metric (3) examines the propagation of false routes and the potential impacts that are not shown by metric 1. Combining metric 2 and 3, we can examine the efficiency of the attacks.

B. Simulation condition one

Under condition one, all connections have different sources and use node 29 as the destination. Node 5 is the malicious host. In AODV, it sends false RREP to every RREQ that it receives. In DSDV, it sends false routing information about node 29 in the routing update packets. We study the selected parameters against the number of connections. Because there are thirty hosts in the network, the maximum number of connections from different sources to node 29 is twenty-eight (except node 5 and 29). The maximum speed of host movement is 5m/s. And the interval between the host reaches current destination and it moves to the next one is 10 seconds. Every point in the figures is the average value of ten simulation scenarios. To calculate the number of hosts getting cheated by the false routes, the routing trees to node 29 is examined every 50 seconds. Figure 1, 2, 3 and 4 show the simulation results.

Figure 1 shows the delivery ratio versus the number of connections to node 29 under three conditions in both protocols: when node 5 does not conduct attacks, when it attacks the routes with false distance vector, and when it attacks the routes with false destination sequence. From figure 1 it is easy to tell that the impact of false destination sequence attack on delivery ratio is much more severe than that of false distance vector attack. The reason is that both AODV and DSDV prefer fresh routes to short ones.

When the malicious host conducts false distance vector attacks, we find that in both protocols the delivery ratios drop to around 50% to 60%. It is determined by the characteristic of distance vector mechanism. If the attacker can accurately predict the sequence number of node 29, the probability that a host will be cheated depends on the probability that it is closer to the attacker than to the victim. In this test environment, it is 50% because the movement of every host is independent. Because we apply a conservative method to predict the sequence number of the victim to avoid the confusion with false destination sequence attacks, the delivery ratio is a little higher than 50%.

The obvious difference between the delivery ratios of ADOV and DSDV when they are under false destination sequence attacks is caused by the implementation of the attacker behaviors. In AODV, the malicious host will add a constant value to the sequence number carried in corresponding RREQ and use the result as the sequence in false RREP. We choose the constant as 2 in the simulation. So there are chances that the false sequence cannot beat the real number. In DSDV, once the false sequence has been established, the attacker will continuously send out new packets to update the value. So more hosts will be cheated. If in AODV the attacker uses a very large number as the false sequence (e.g. 0x7fffffff), we would expect a lower delivery ratio. Therefore, AODV is not more resistant to false destination sequence attacks than DSDV.

One interesting point, when AODV is under attacks on destination sequence, is that the delivery ratio will increase a little as the number of connections increases. It happens because the attacker does not apply any intelligent destination sequence prediction methods but only adding a constant to the sequence in RREQ. As the number of connections increases, the true sequence increases faster, and the probability that the chosen fake sequence is smaller than the real value also increases. Thus less traffic will be attracted to the attacker.

Figure 2 shows the number of hosts that are cheated by the false routes versus the number of connections. In DSDV, the number of hosts that are cheated does not vary a lot as the number of connections changes because of the proactive property. When false distance vector attacks are conducted, less than half of the hosts are cheated. But when the network is under false destination sequence attacks, almost all hosts are cheated. In AODV, as the number of connections increases, more false RREPs will be sent by the attacker. Therefore, more normal hosts will be cheated. Both protocols prefer the routes with larger sequence, so the false destination sequence attacks cheat much more hosts. We assume that the hosts are uniformly distributed in the test area so there are about half of the hosts are closer to the attacker than to the destination. They will be cheated by the false distance vector attacks if the sequence number in false routes is the same as in the real ones. Because the attacker applies a conservative sequence prediction method, there are less than 50% of the hosts are cheated in both protocols. But the false destination sequence attacks can cheat all hosts except the real destination if the false sequence number is selected large enough.

Figure 3 shows the communication overhead of the two attacks in AODV and DSDV. The number of false route updates sent in DSDV does not change a lot because of the proactive property. And the overhead of conducting two attacks does not show big difference. In AODV every false RREP can only attack one RREQ, so the number of false RREPs sent by the attacker is roughly proportional to the number of connections. The two curves of AODV are very close to each other but the one for false destination sequence attacks is a little higher. On one hand, it shows that both attacks put similar traffic overhead on the attacker. On the other hand, the false sequence numbers generated by the attacker in AODV disturb the updates of real numbers and introduce more route queries into the system.

Figure 4 examines the efficiency of the two attacks in both protocols. It shows the number of hosts got cheated versus the number of false route packets sent by the attacker. For DSDV, the values form two group of points which are very close to each other. They can be derived from the curves shown in figure 2 and 3. For AODV, the curves are very similar to the lines in figure 2 because the number of false RREPs sent by the attacker is roughly proportional to the number of connections. Sending the same number of false routes, false distance vector attacks in AODV cheat more hosts than in DSDV. The reason is that from the broadcast RREQ packets, the attacker can more accurately know the sequence number of the victim.

From figure 1 to figure 4, we can tell that the attacks on destination sequence and the attacks on distance vector have about the same communication overhead but the former has more severe impacts. For the intrusion prevention and intrusion detection systems designed to protect ad hoc networks using AODV or DSDV, this kind of attack should be considered first.

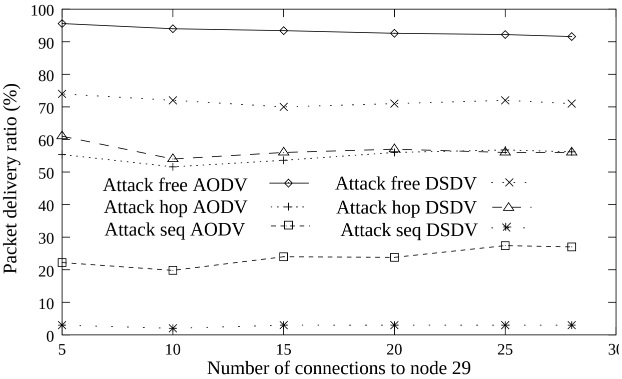

Fig. 1 The delivery ratio versus the number of connections to node 29

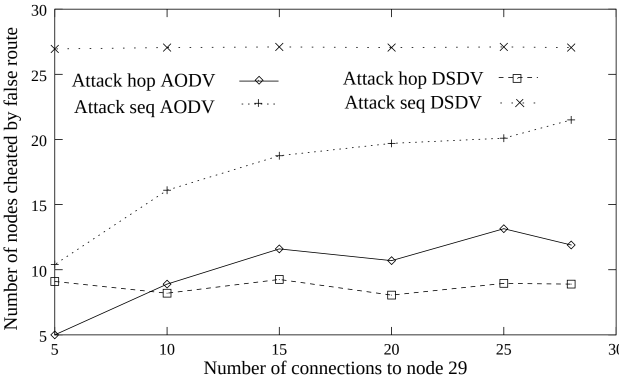

Fig. 2 The number of hosts that are cheated versus the number of connections to node 29

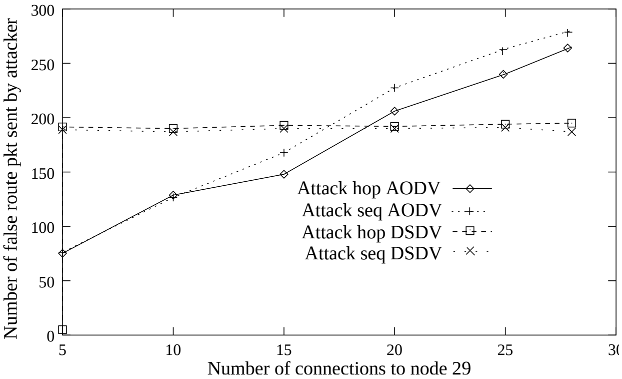

Fig. 3 The number of false routing packets sent by the attacker versus the number of connections to node 29

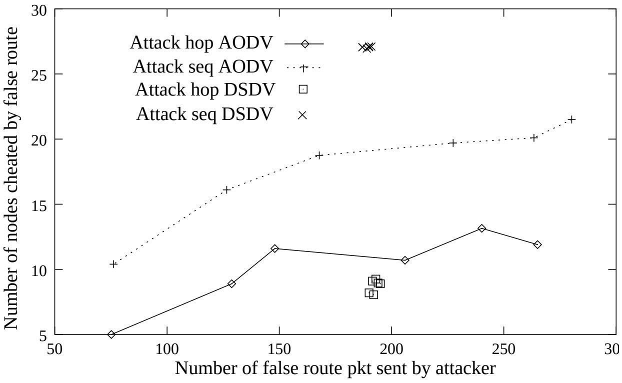

Fig. 4 The number of hosts that are cheated versus the number of false routing packets sent by attacker

C. Simulation condition two

Under condition two, we generate a connection scenario in which each of the twenty-nine normal hosts is the source and the destination of one connection. Node 5 is the attacker. We study the selected parameters versus the mobility of the hosts, which is represented by the maximum moving speed. The results are given out in figure 5 and 6.

Figure 5 shows the delivery ratio versus the maximum speed of hosts under the conditions the same as figure 1. The delivery ratio of attack free condition in AODV does not vary a lot, which shows that the mobility of host is still within the suitable serving range of AODV. In DSDV, the delivery ratio of attack free condition decreases as the maximum speed increases, which shows that DSDV is more sensitive to the mobility of the hosts. When the protocols are under attack, the delivery ratio only fluctuates within a small range. This is because the route changes caused by host movement put challenges on both the normal hosts and the attacker. At one hand, the broken routes lead to the drop of packets. On the other hand, because of the break of false routes, the normal hosts have chance to construct the paths not passing through the malicious host. They take effects at the same time and keep the delivery ratio roughly stable. Compared to figure 1, we find that more data packets successfully reach to the destinations in AODV when the network is under attack. This can be explained by the difference between the connection scenarios of the two test cases. Under condition two, every host is the source of one connection, and it may broadcast the RREQ throughout the network. Other hosts can establish the routes through the paths that they receive the request. Therefore, many hosts do not have to listen to the false RREPs sent by the attacker. More safe routes are set up and the delivery ratio is higher.

Figure 6 shows the number of routing packets sent by node 5 when it behaves properly and when it conducts the attacks. In DSDV, the curves are very close to each other because the attacker can carry multiple false routes in the same routing packet. It does not have to increase the frequency of sending route update. In AODV the attacker will send five to ten times more RREP when it attacks every RREQ it receives. If the mobile hosts monitor the nearby traffic, this anomalous increase can be used as the pattern to activate IDS to examine possible attacks.

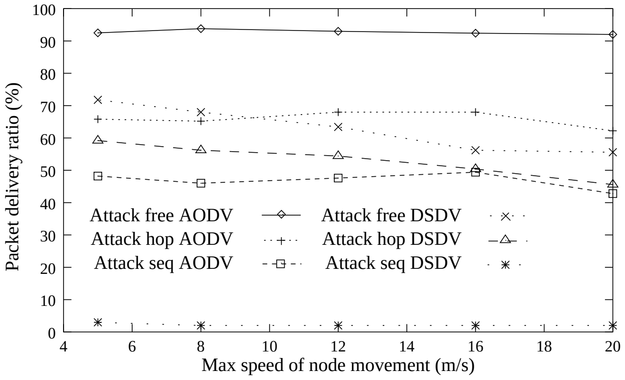

Fig. 5 The delivery ratio versus the maximum speed of hosts.

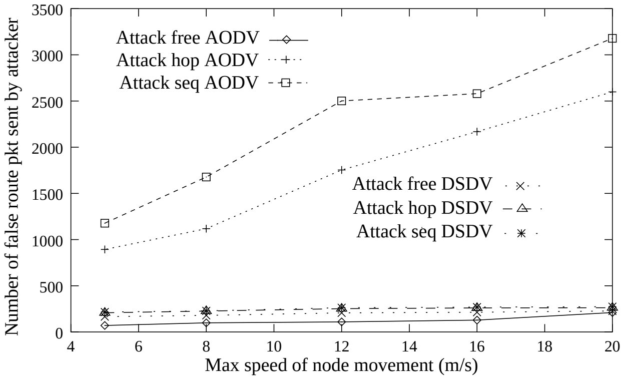

Fig 6 The number of routing packets sent by node 5 versus the maximum speed of hosts

VI. Detecting False Destination Sequence Attacks

When the malicious hosts introduce false information into the networks, their behaviors and the conflicts between false and true information form special patterns, which can be used to detect the attacks. In addition, the connectivity history and the propagation paths of the false information can be used to identify the sources of attacks. Our research on security in ad hoc networks [36] [32] tries to collect information and patterns of attacks and to provide the guidelines for the design of the intrusion detection systems. An example of detecting false destination sequence attacks in AODV and DSDV is given out below.

From the simulation results, we find that the attack on destination sequence can cheat a large part of the hosts and severely impact the delivery ratio. To "beat" other available routes, the attacker must choose a large number as the false sequence to show its "freshness". The false number will be larger than the sequence generated by the victim. If the victim host can find this false sequence number, it will detect the attack. In DSDV the false sequence route will be transferred to all directions. There exists upper limit of delay that the false route will reach to the victim if it is connected to the attacker and the false sequence always outruns the real one. In AODV, only when a host on the false route moves out of the range of its neighbor, the re-initiation procedure of the source will send out RREQ that carries the false sequence. Because the RREQ is broadcast throughout the network, there is a good chance that the real destination will receive the request. If the false sequence is still larger than the real one, the host detects the attack. The detection of false destination sequence attacks in AODV heavily depends on the mobility of hosts. Therefore, no upper limit of delay between the attack is conducted and it is detected can be guaranteed.

A host can find its destination sequence in the routing packets sent by other hosts. Under the normal operation of AODV and DSDV, the destination sequence carried in the packets can never be larger than the real sequence plus one. But when the host is under attack on destination sequence, the difference between the received and local sequence numbers will be equal or larger than 2. Figure 7 and 8 give out the difference between the two sequence numbers detected by a normally behaved host in 1000 second simulation time. The routing packets are coming from different hosts. In DSDV, when the false sequence is larger than the real number, it can be detected in any route update sent by a neighbor of the victim. If the real number is larger, the attacker will find it and conducts the new attack. Therefore we can find the difference fluctuates between 0 and 2. In AODV, the normal host detects eleven times that the incoming sequence number is larger than local number plus one.

In both protocols some attacks are not detected. Two problems that impact the detection of false destination sequence attacks in AODV and DSDV are: (1) The real sequence may outrun the false one when it is received by the victim. Then the host cannot find that the false number is not generated by it. (2) A tighter limit of the delay between the false sequence is generated and it reaches the victim, if they are connected, should be achieved. We are working on these problems. A protocol that uses one detected attack to activate the detection of other attacks has been designed in AODV [33]. The basic idea is to re-examine all routing information coming from the same sources and activate the re-initiation. A software module that can be integrated into AODV and DSDV to increase the accuracy of detecting the attacks is under construction.

Collecting and determining the anomaly patterns of attacks is a challenging topic in IDS for ad hoc networks and is still under research. The example provided above shows that combining protocol analysis and practical simulation

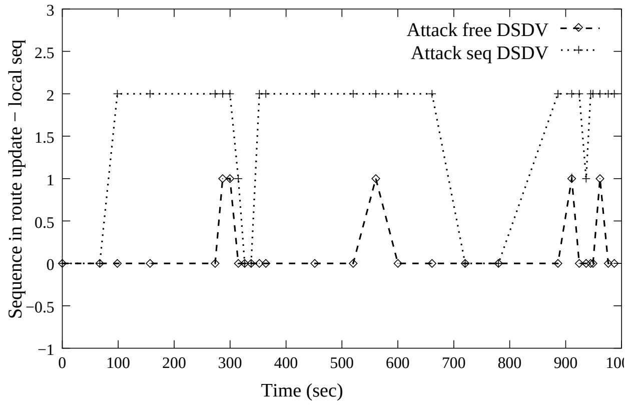

Fig. 7 The difference between two sequences when the host is under false sequence attacks (DSDV)

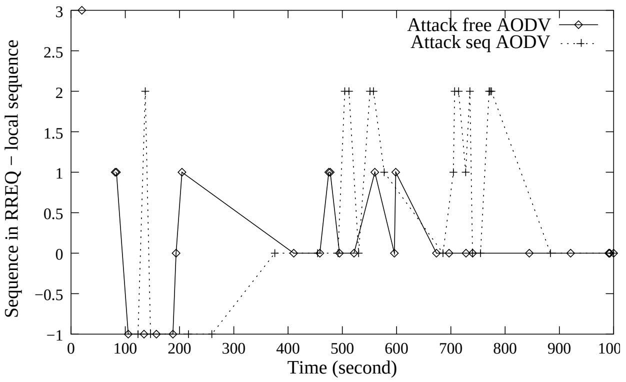

Fig. 8 The difference between two sequences when the host is under false sequence attacks (AODV)

may accelerate this procedure. We plan to apply this mechanism to the establishment of our IDS and the design of a secure routing protocol.

VII. Conclusions

The security of the ad hoc network routing protocols is still an open problem and deserves more research work. This paper studies the vulnerabilities and attacks on two of the protocols – AODV and DSDV. The analysis shows that as AODV provides fair performance with reasonable overhead and adaptability to both traffic load and host mobility, the on-demand property also introduces some security deficiencies. It allows the malicious host to attack the network in real time with flexibility. It is more difficult to locate the sources of the false information because of the unicast of false reply. The proactive property also has disadvantages. The routine exchange of routes in DSDV enables the false routing information to propagate within a wider range. The malicious host can conduct multiple attacks in the same routing packet. Because both protocols prefer the fresh routes which are identified by large sequence numbers, the attacks on destination sequence have more severe impacts on packet delivery ratio than the attacks on distance vector. The attacks may lead to the confusion on network connectivity, thus degrading the performance of the networks.

The simulation results of selected parameters in different connection scenarios support our analyses. The delivery ratio curves show that the attacks on sequence will attract more packets to the malicious host. False distance vector attacks will cheat less than 50% of the hosts in a uniformly distributed network. The communication overhead caused by conducting attacks is more stable on the traffic load and the width of attack in DSDV than in AODV. The analysis and simulation also show that it is more efficient to detect false destination sequence attacks in DSDV than in AODV.

The research to protect wired network routing protocols [37] has shown that it is the property, instead of the protocol detail, that leads to the security deficiencies. The example attacks on AODV and DSDV can also be applied to attack other protocols sharing the properties. Thus the analysis results and anomaly patterns of the attacks can be employed to prevent or detect the coterminous attacks on different protocols. Because the primary different between AODV and DSDV is the on-demand and proactive properties, we may generalize the analysis to other on-demand or proactive protocols.

There are many problems to be solved in protecting the ad hoc networks. We plan to study the relationship between the average delay of detecting false sequence attacks and the mobility of the hosts. We will design an efficient mechanism which can be smoothly integrated into current protocols to establish safe routes when false routing information is discovered. We plan to study more features of the routing protocols to exploit their security deficiencies. On achieving the secure distribution of individual intrusion detection results, we plan to establish the trust relation among hosts in the open area of ad hoc networks [38]. The results will provide the guidelines for the design of a secure ad hoc routing protocol and become the building blocks of an IDS for ad hoc networks.

References

[1] C. Perkins and E. Royer, “Ad-Hoc On-Demand Distance Vector Routing,” in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, 1999.

[2] D. Johnson and D. Maltz, *Dynamic Source Routing in Ad Hoc Wireless Networks*, Kluwer Academic Publisher, 1996.

[3] V. Park and M. Corson, "A highly adaptable distributed routing algorithm for mobile wireless networks," in *Proceedings of IEEE InfoComm*. IEEE, 1997.

[4] C. Perkins, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *Proceedings of SIGCOMM*, 1994.

[5] C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," in *Proceedings of IEEE SICON*, 1997.

[6] S. Murthy and J. Aceves, "An efficient routing protocol for wireless networks," *Mobile Networks and Applications*, vol. 1, no. 2, pp. 183–197, 1996.

[7] Z. Haas and M. Pearlman, "The zone routing protocol (ZRP) for Ad Hoc networks," IETF Internet Draft, Version 4, July, 2002.

[8] T. Camp, J. Boleng, B. Williams, L. Wilcox, and W. Navidi, "Performance comparison of two location based routing protocols for Ad Hoc networks," in *Proceedings of the IEEE INFOCOM*, 2002.

[9] Z. Haas, J. Halpern, and L. Li, "Gossip-based Ad Hoc routing," in *Proceedings of the IEEE INFOCOM*, 2002.

[10] C. Perkins, E. Royer, and S. Das, "Performance comparison of two on-demand routing protocols for Ad Hoc networks," in *Proceedings of IEEE INFOCOM*, 2000.

[11] S. Das and R. Sengupta, "Comparative performance evaluation of routing protocol for mobile, Ad Hoc networks," in *Proceedings of IEEE the Seventh International Conference on Computer Communications and Networks*, 1998.

[12] L. Venkatraman and D. Agrawal, "Authentication in Ad Hoc networks," in *Proceedings of the 2nd IEEE Wireless Communications and Networking Conference*, 2000.

[13] P. Nikander, "Authentication, authorization, and accounting in Ad Hoc networks," in *Proceedings of the Helsinki University of Technology Seminar on Internetworking*, 2000.

[14] Y. Zhang and W. Lee, "Intrusion detection in wireless Ad-Hoc networks," in *Proceedings of ACM MobiCom*, 2000.

[15] Z. Zhou and Z. Haas, "Secure Ad Hoc networks," *IEEE Networks*, vol. 13, no. 6, pp. 24–30, 1999.

[16] V. Bharghavan, "Secure wireless LANs," in *Proceedings of the ACM Conference on Computers and Communications Security*, 1994.

[17] H. Yang, X. Meng, and S. Lu, "Self-organized network-layer security in mobile ad hoc networks," in *Proceedings of ACM MOBICOM Wireless Security Workshop (WiSe)*, 2002.

[18] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Self-organized public-key management in ad hoc wireless networks," in *Proceedings of ACM MOBICOM Wireless Security Workshop (WiSe)*, 2002.

[19] P. Papadimitratos and Z. Haas, "Performance evaluation of secure routing for mobile ad hoc networks," in *Proceedings of ACM MOBICOM Wireless Security Workshop (WiSe)*, 2002.

[20] P. Sinha, R. Sivakumar, and V. Bharghavan, "Enhancing Ad-Hoc routing with dynamic virtual infrastructures.," in *Proceedings of IEEE INFOCOM*, 2001.

[21] S. Bhargava and D. Agrawal, "Security enhancements in AODV protocol for wireless Ad Hoc networks," in *Proceedings of Vehicular Technology Conference*, 2001.

[22] P. Papadimitratos and Z. Haas, "Secure routing for mobile Ad Hoc networks," in *Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*, 2002.

[23] P. Albers and O. Camp, "Security in Ad Hoc network: A general ID architecture enhancing trust based approaches," in *Proceedings of International Conference on Enterprise Information Systems (ICEIS)*, 2002.

[24] R. Ramanujan and R. Edin, "TIARA: Techniques for intrusion-resistant Ad Hoc routing algorithms," DARPA funded proposal, www.oracorp.com/projects/current/tiara.html, 2000-2003.

[25] Z. Haas, "Secure communication for Ad Hoc networking," NSF funded proposal, http://wnl.ece.cornell.edu/wnlprojects.html, 2000-2003.

[26] D. Agrawal, "On robust and secure mobile Ad Hoc and sensor netwroks," NSF funded proposal, http://www.ececs.uc.edu/ cdmc/, 2001-2004.

[27] Wenke Lee, "CAREER: Adaptive intrusion detection systems," NSF funded proposal, http://www.cc.gatech.edu/ wenke/, 2002-2005.

[28] E. Royer and C. Perkins, "Multicast operation of the Ad Hoc on-demand distance vector routing protocol," in *Proceedings of MobiCOM*, 1999.

[29] M. Marina and S. Das, "On-demand multipath distance vector routing in Ad Hoc networks," in *Proceedings of IEEE International Conference on Network Protocols (ICNP)*, 2001.

[30] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, 1999.

[31] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An on-demand secure routing protocol resilent to Byzantine failures," in *Proceedings of ACM MOBICOM Wireless Security Workshop (WiSe)*, 2002.

[32] W. Wang, Y. Lu, and B. Bhargava, "On vulnerability and protection of Ad Hoc On-demand Distance Vector Protocol," To appear in the proceedings of 10th IEEE International Conference on Telecommunication (ICT), 2003.

[33] W. Wang, Y. Lu, and B. Bhargava, "Intruder identification in ad hoc on-demand distance vector protocol," Technical report, Department of Computer Sciences, Purdue University, 2002.

[34] M. Grossglauser and D. Tse, "Mobility increases the capacity of Ad-hoc wireless networks," in *Proceedings of INFOCOM*, 2001.

[35] "http://www.isi.edu/nsnam/ns/," Sep, 2002.

[36] B. Bhargava, "Trusted routing and intruder identification in mobile Ad Hoc networks," CERIAS funded proposal, 2002-2003.

[37] S. Bellovin, "Security problems in the TCP/IP protocol suite," *Computer Communications Review*, vol. 19, no. 2, pp. 32–48, April 1989.

[38] B. Bhargava and Y. Zhong, "Authorization based on evidence and trust," in *Proceedings of Data Warehouse and Knowledge Management Conference (DaWak), France*, 2002.